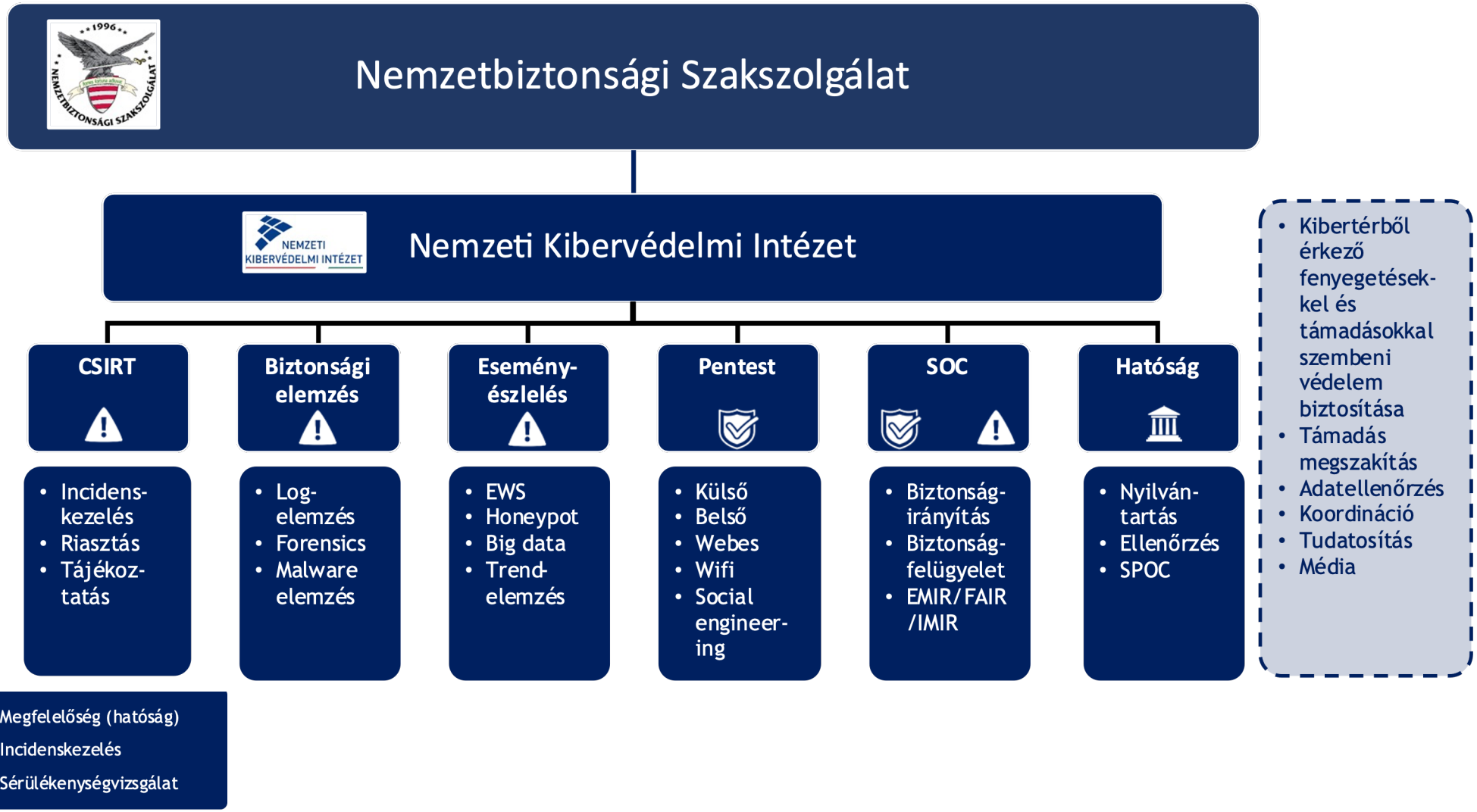
NEMZETI KIBERVÉDELMI INTÉZET

A Nemzeti Kibervédelmi Intézet (NKI) feladatai - érdekes esetek a közelmúltból

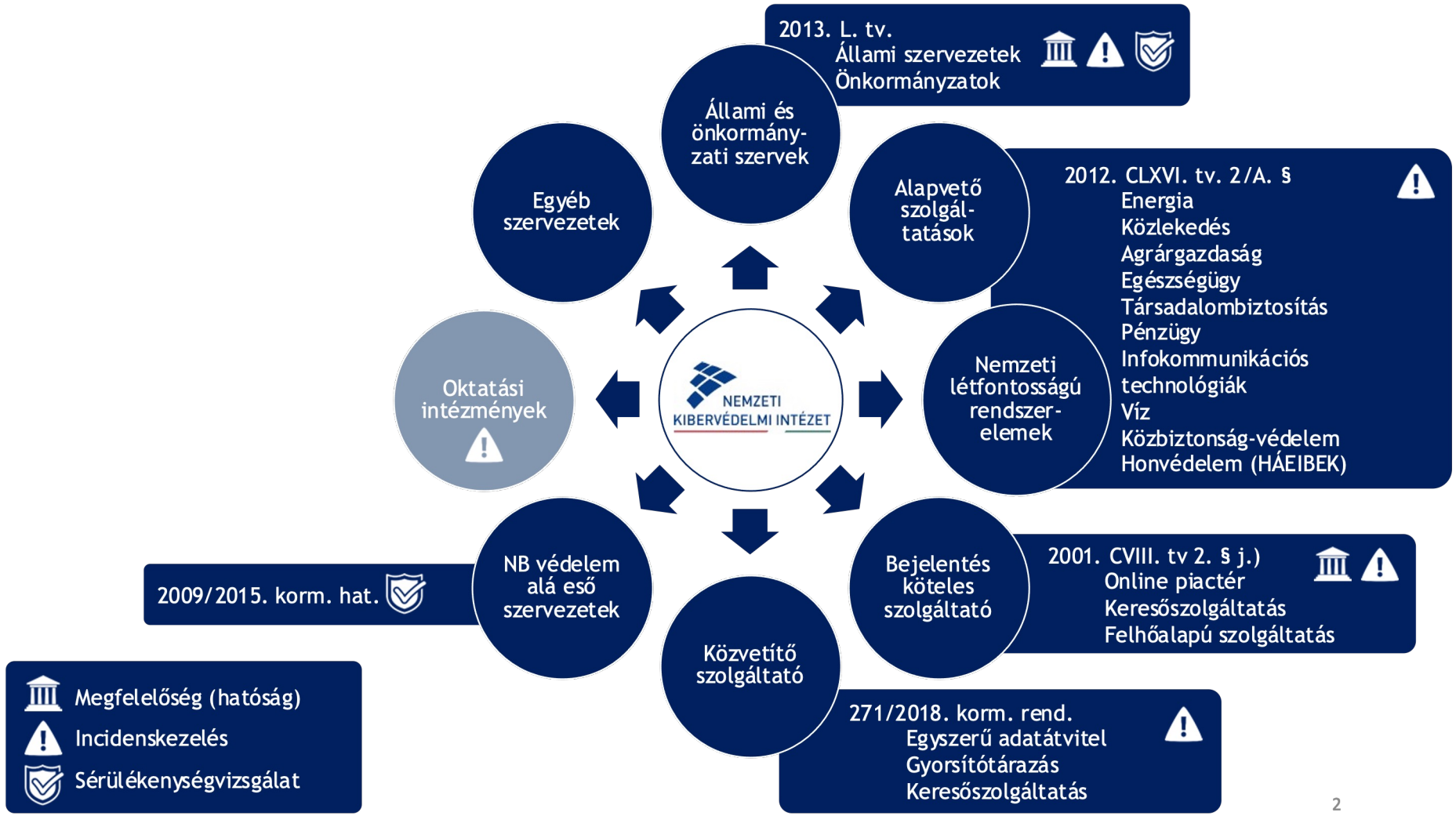
Marsi Tamás

2022. – Debrecen EIVOK

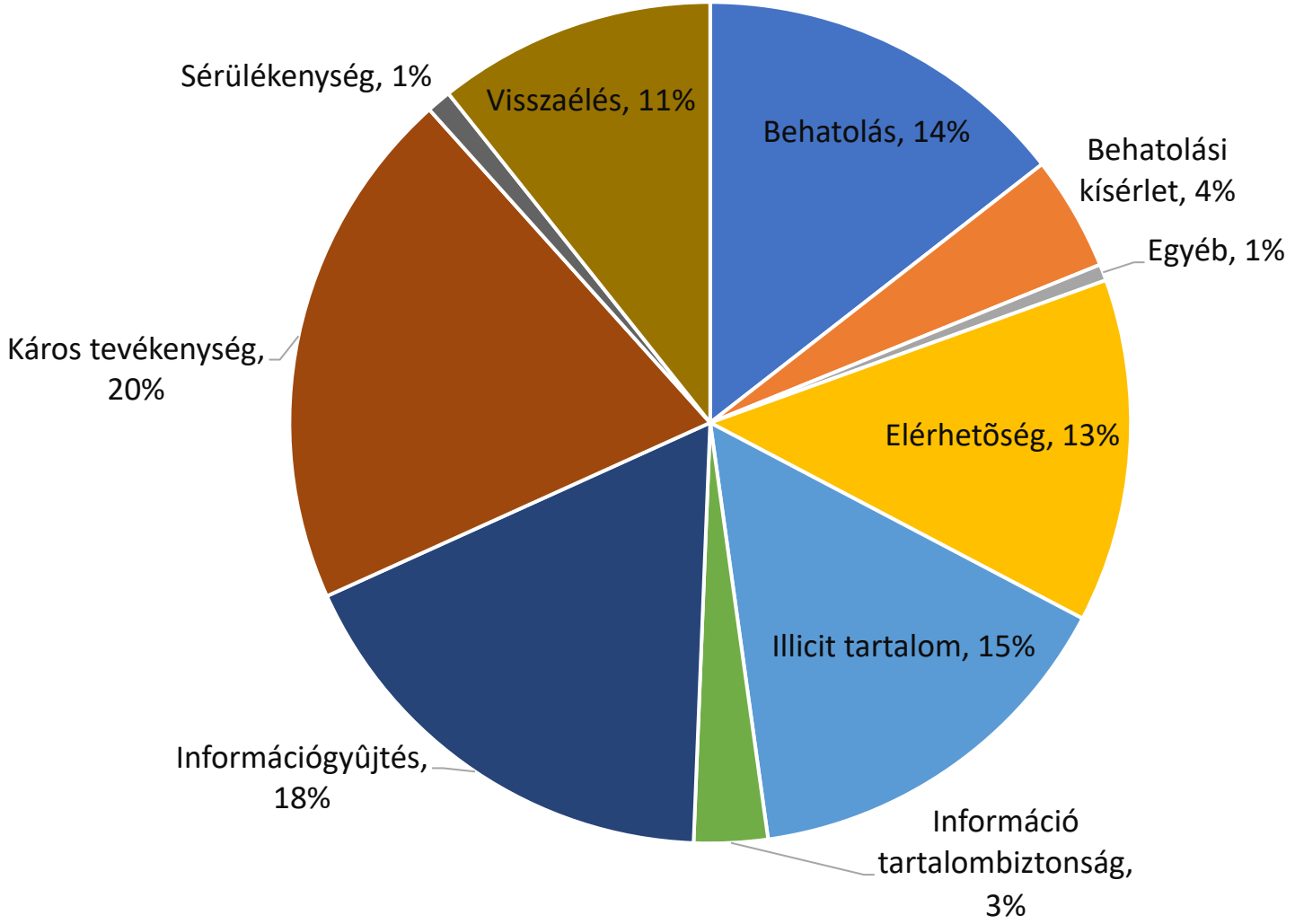
NKI felépítése



NKI ügyfélköre



Statisztika

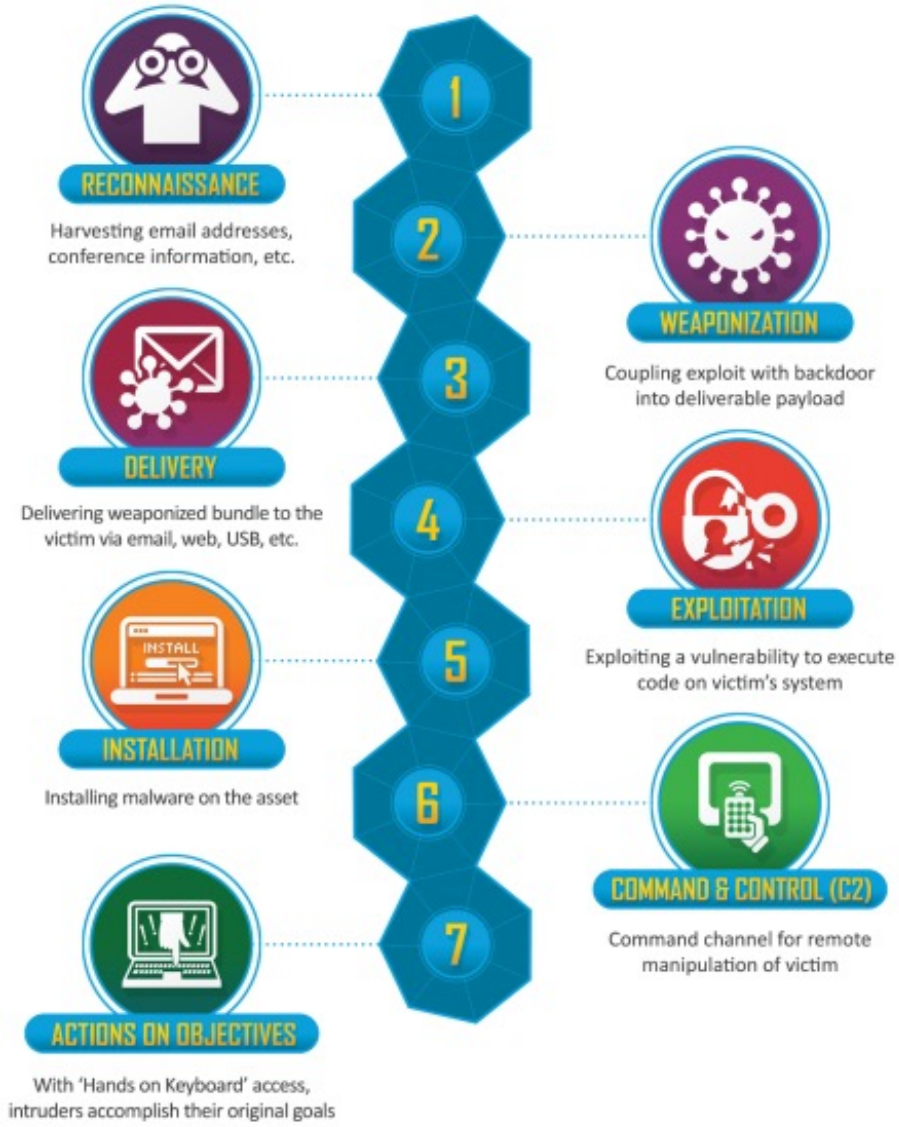


Támadók motivációi

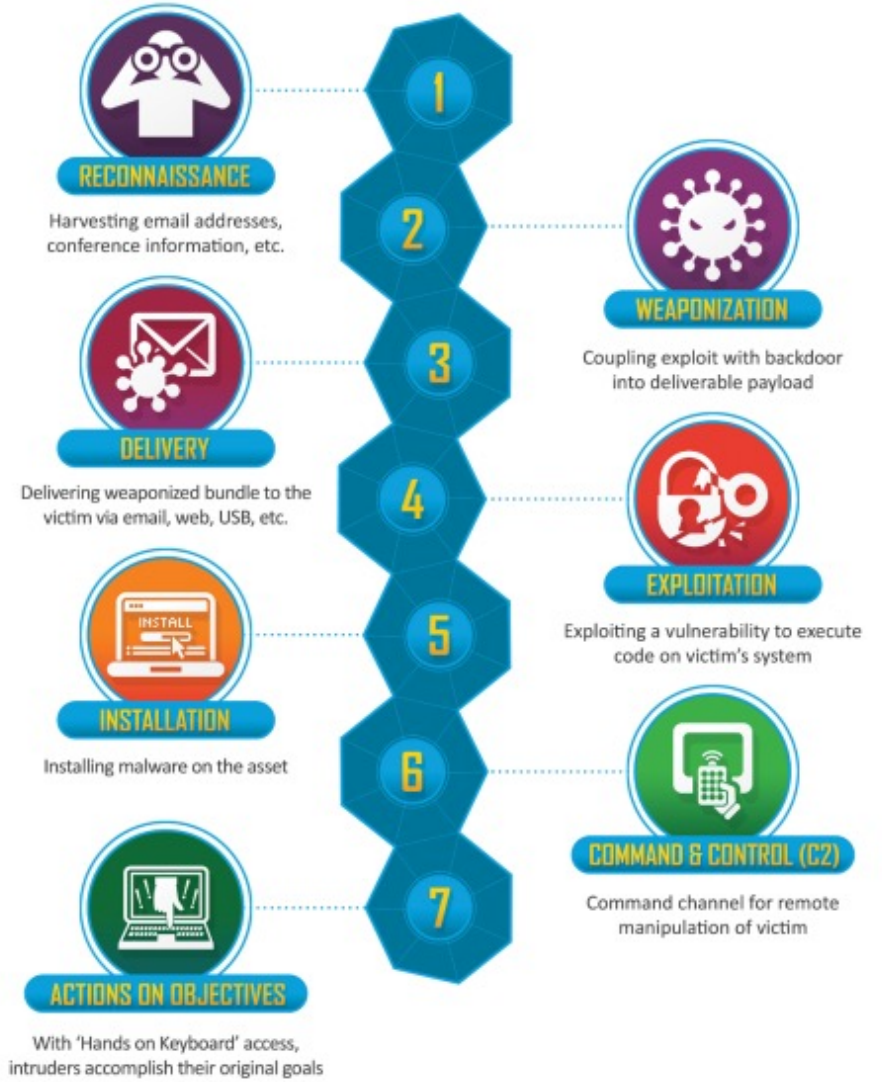
- Script kiddie
  - Cél: Hírnév, feltűnés, pénz
- Hacktivizmus
  - Ideológiai motiváció
  - Ideológia közvetítése
- Kiberbűnözés
  - Cél: közvetlen anyagi haszonszerzés
  - Pénzügyi és személyes adatok megszerzése
- Kiberkémkedés
  - Más országok politikai, gazdasági befolyásolása
  - Szofisztikált támadások
  - Cél: információ

Cyber killchain

1. Előkészítés
   - Kutatás
   - Azonosítás
   - Támadók kiválogatása
   - Profilozés
2. Felfegyverzés
   - Tervezés, eszköz létrehozés
   - Malware hozzáillesztése a célba juttató eszközhöz (Word, PDF)



Cyber killchain



3. Célba juttatás
   - Pendrive, e-mail
   - Ami ellen kevéssé védekeznek
4. Exploitálás
   - Kód triggerelése
   - Sérülékenységek kihasználása
5. Installálás
   - Backdoor telepítése
   - Perzisztencia kiépítése
   - Álcázás

Cyber killchain

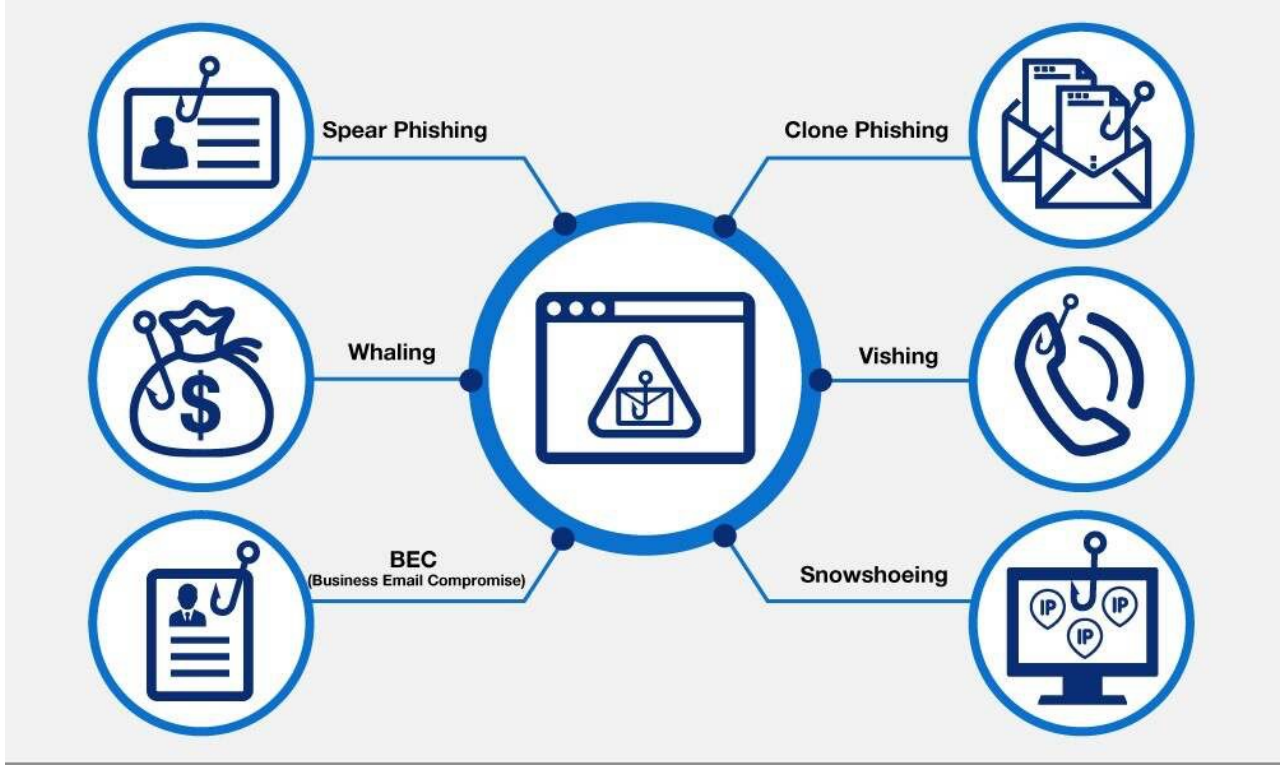
6. C&C kommunikáció
    Külső elérés biztosítása
    Láthatatlanság biztosítása
7. Konkrét lépések
    Adatok elérése
    Célok elérése
        Keylogging, szivárogtatás
    Másik célpont keresése, találása
    Hosszú ideig jelenlét biztosítása

Adathalászat

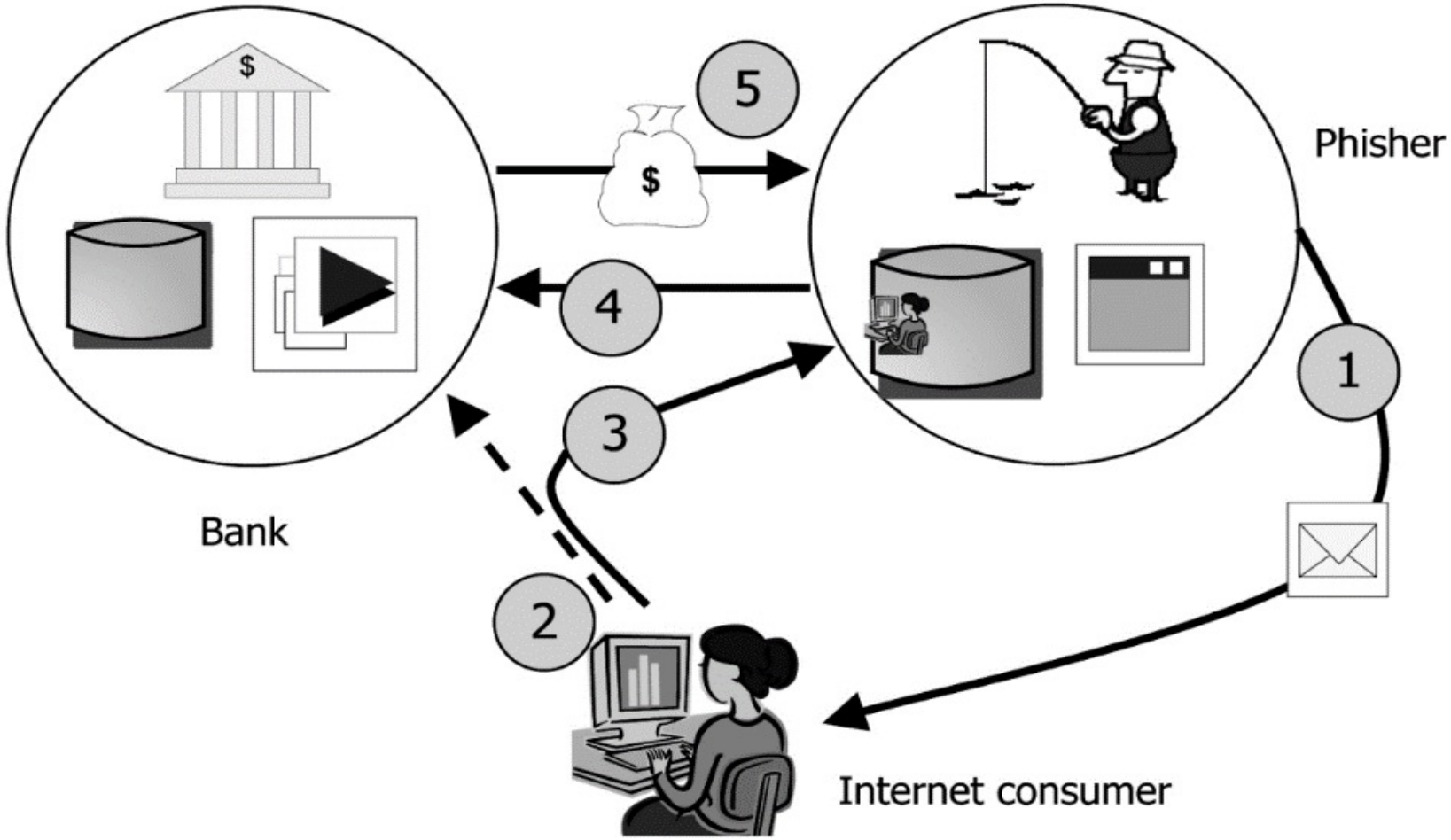
- Célja
  - Azonosítók (felhasználónevek, jelszavak) megszerzése
- Módja
  - E-mail
  - Internetes űrlap
  - (Telefon)
- Levelek természete
  - Minőségük eltérő
  - A cél általában adathalászat
  - Általában nem célzott támadás
  - Forrás beazonosítása nehézkes

Adathalászat típusok

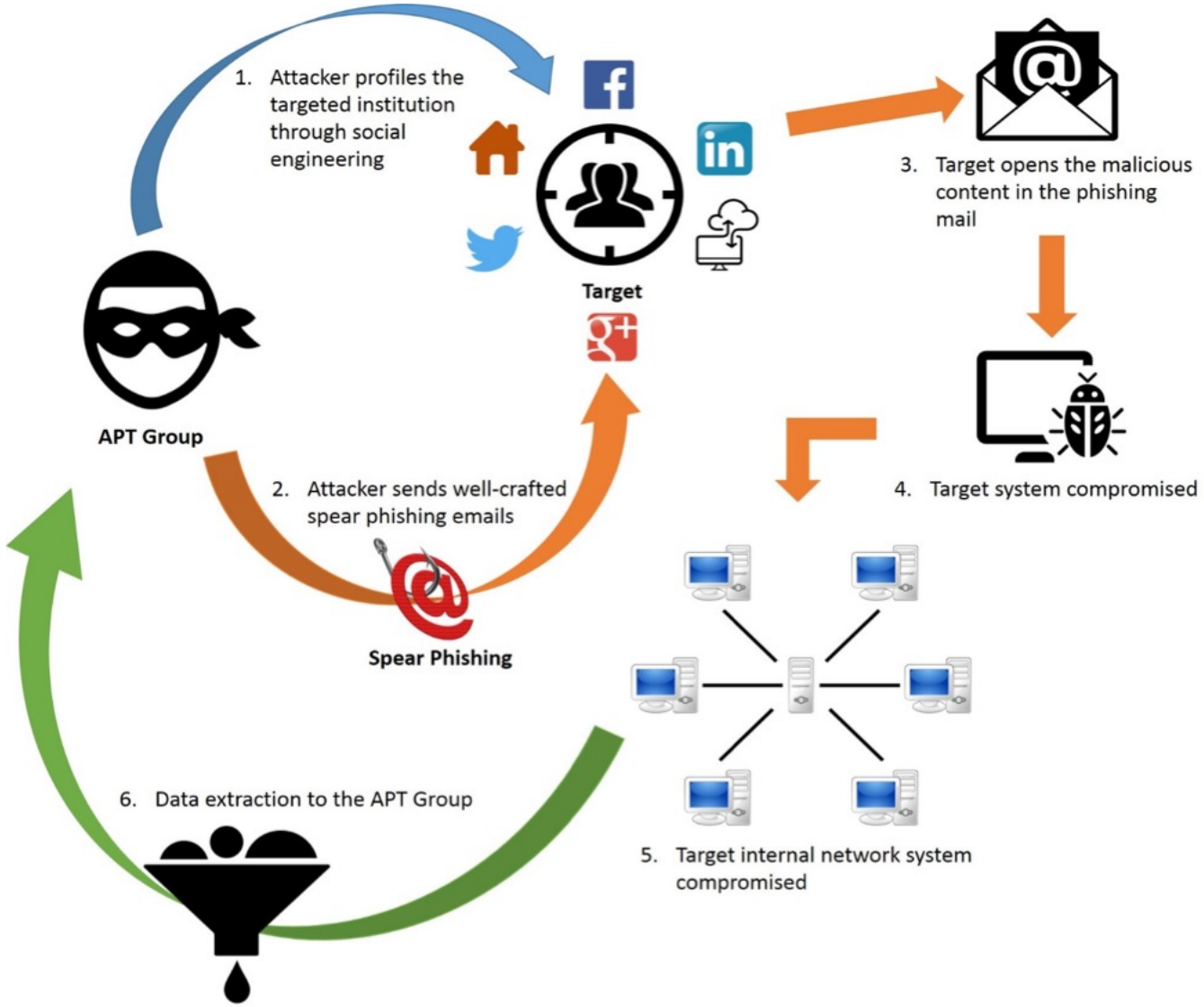
- Célzott adathalászat
- Bálnavadászat
  - CEO
- Business Email Compromise
  - Alternatív bankszámlára kér pénzt
- Klónozás
- Hangos csalás (Voice phishing)
- Hópihe
  - Spam filterek kijátszása kevés email küldésével



Adathalászat séma



Célzott adathalászat séma



Nigériai csalás

Cs 2018.10.18. 0:43

Jean-Pierre Owaoma <jpierreo0021@gmail.com>

Üdvözlet,

Címzett

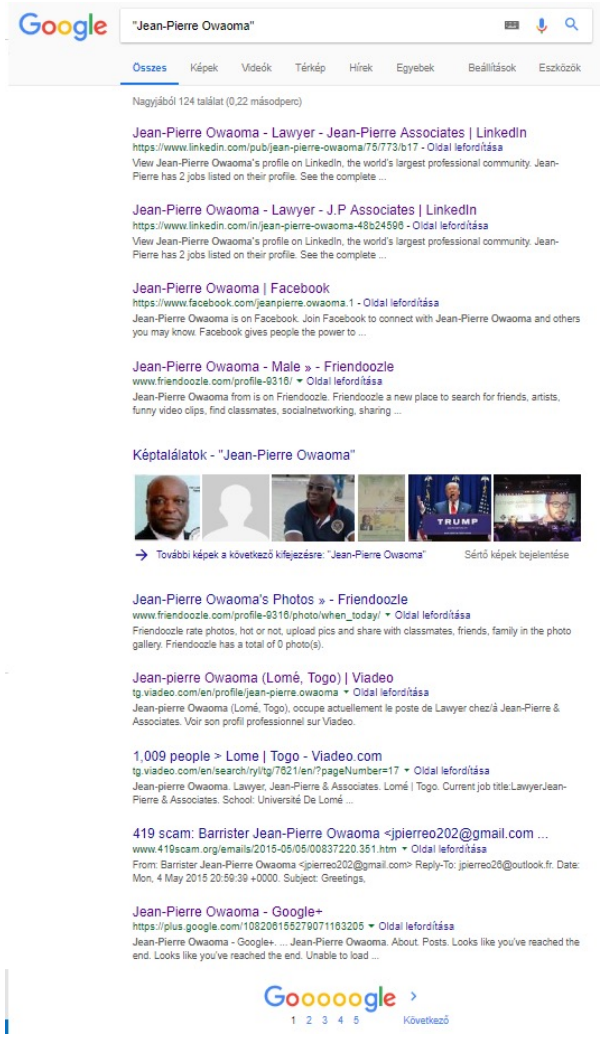
Eltávolítottuk a fölösleges sortöréseket az üzenetből.

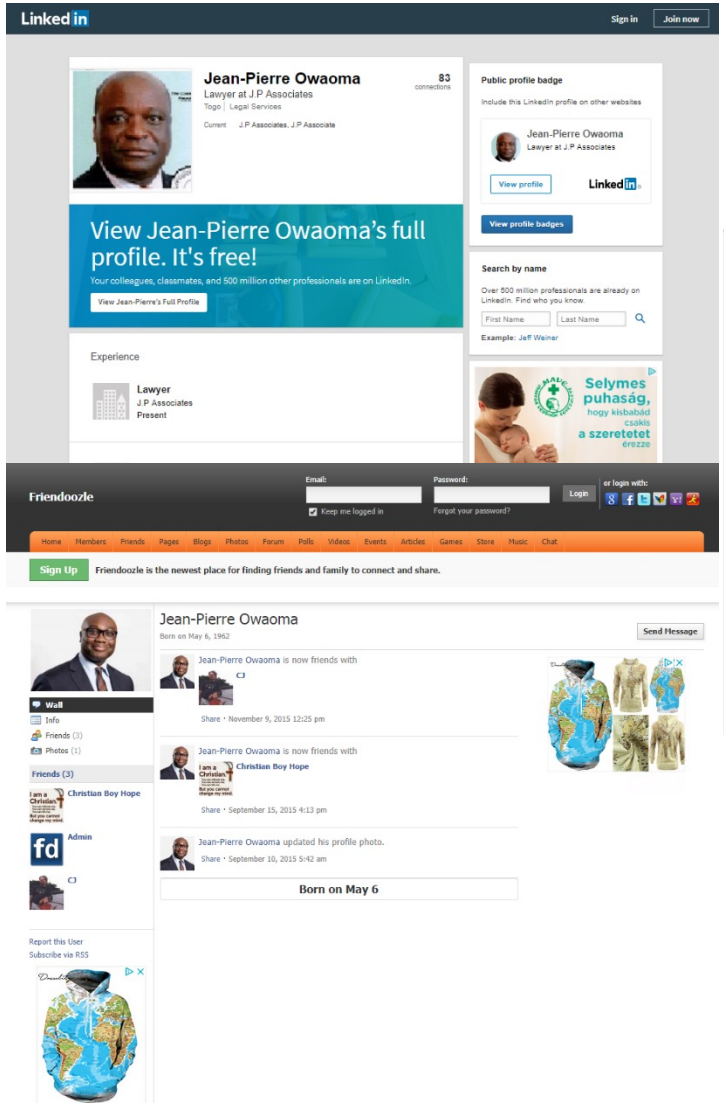
Üdvözlet,

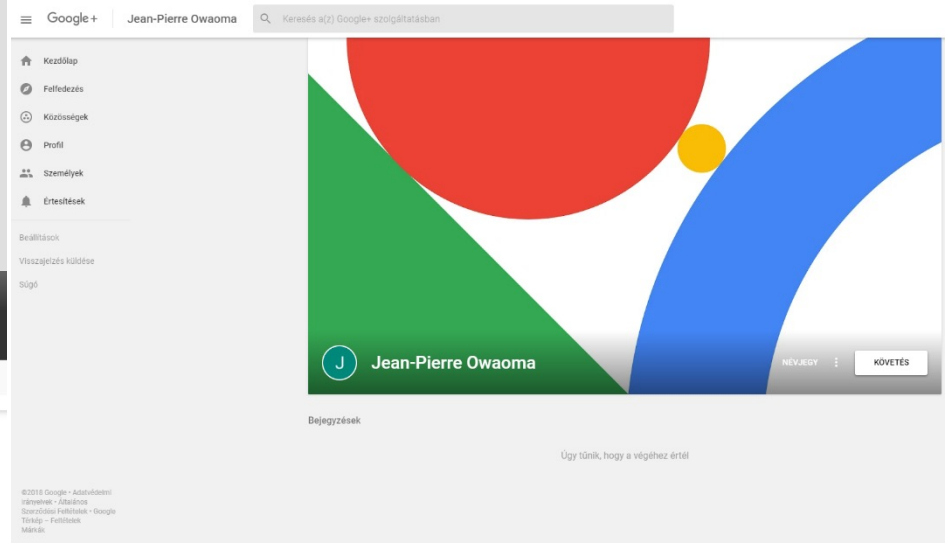
Kérlek, nagyon sajnálom, hogy zavarlak. Én azonban Jean-Pierre Owaoma vagyok, én vagyok a személyes ügyvéd egy késő Mr. P.A-nak, az Ön országának állampolgárának, aki itt halt meg az én országomban, a Togói Köztársaságban, és itt egy óriási pénzt hagyott itt egy banknál.
Az összeg 5,7 millió euró. Ha érdekel, hogy segítsek nekem igényelni ezt a pénzt, és küldje el az országomból, kérem, térjen vissza a lehető leghamarabb.

Kösz.
Jean-Pierre Owaoma.

Nigériai csalás







Nigériai csalás

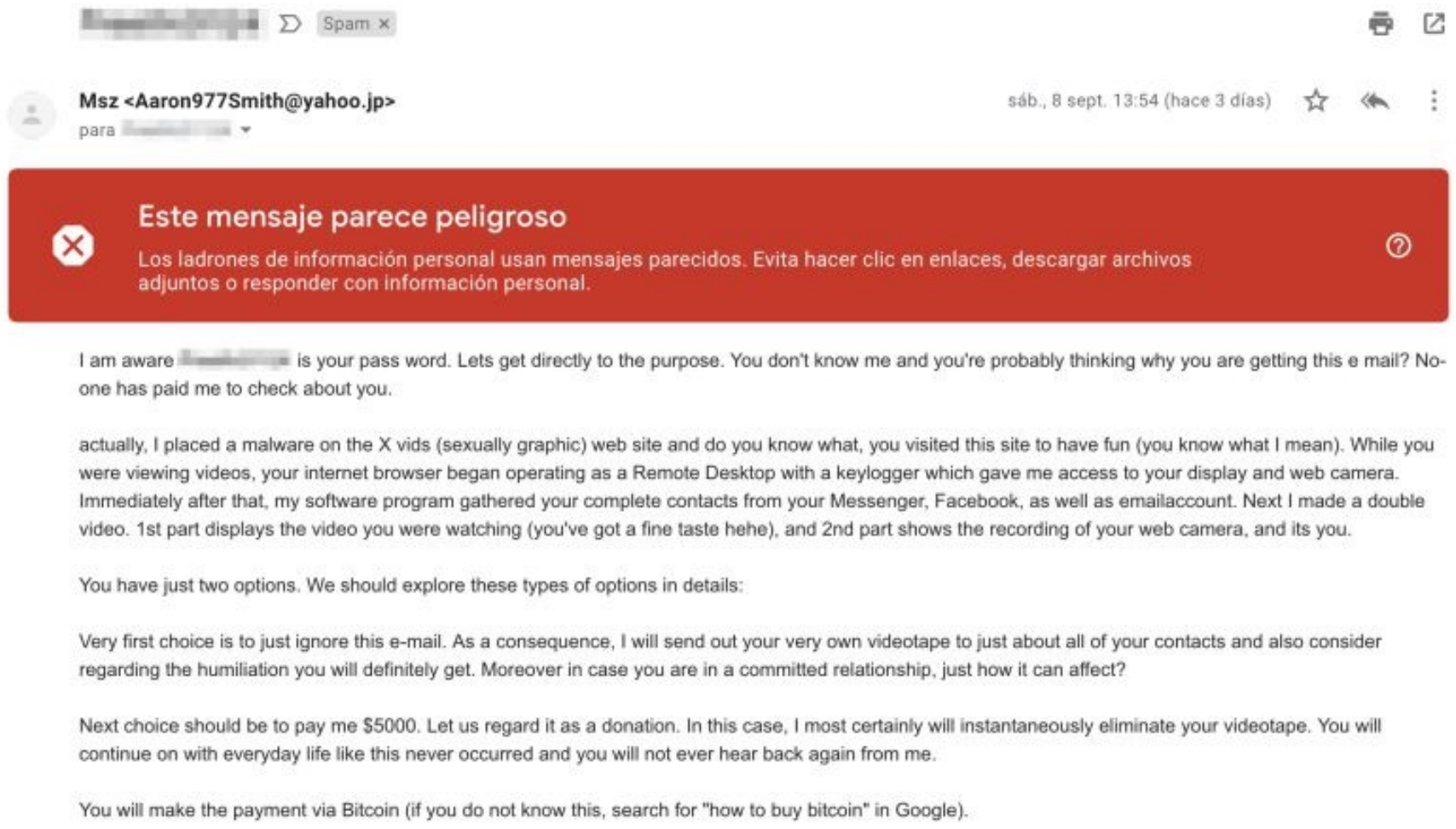
--
Irodánk elérhetősége: 2554 Road Of Kpalime Face Pharmacy Bet, Lome, Gulf.

Ez a WU bank igazgatója értesíti Önt arról, hogy a Nemzetközi Valutaalap (IMF) 850 000,00 USD kártérítést fizet Önnek, mert megtalálta az Ön e-mail címét a csalás áldozatainak listáján. Hajlandó vagy venni ezt az alapot vagy sem?

Sürgősen várjuk a hírt.

Tisztelettel
Tony Albert
BANKIGAZGATÓ
Lépjen kapcsolatba a Whatsappal, +22892905783

Sextortion



[redacted] Spam ×

Msz <Aaron977Smith@yahoo.jp> sáb., 8 sept. 13:54 (hace 3 días)

para [redacted]

Este mensaje parece peligroso

Los ladrones de información personal usan mensajes parecidos. Evita hacer clic en enlaces, descargar archivos adjuntos o responder con información personal.

I am aware [redacted] is your pass word. Lets get directly to the purpose. You don't know me and you're probably thinking why you are getting this e mail? No-one has paid me to check about you.

actually, I placed a malware on the X vids (sexually graphic) web site and do you know what, you visited this site to have fun (you know what I mean). While you were viewing videos, your internet browser began operating as a Remote Desktop with a keylogger which gave me access to your display and web camera. Immediately after that, my software program gathered your complete contacts from your Messenger, Facebook, as well as emailaccount. Next I made a double video. 1st part displays the video you were watching (you've got a fine taste hehe), and 2nd part shows the recording of your web camera, and its you.

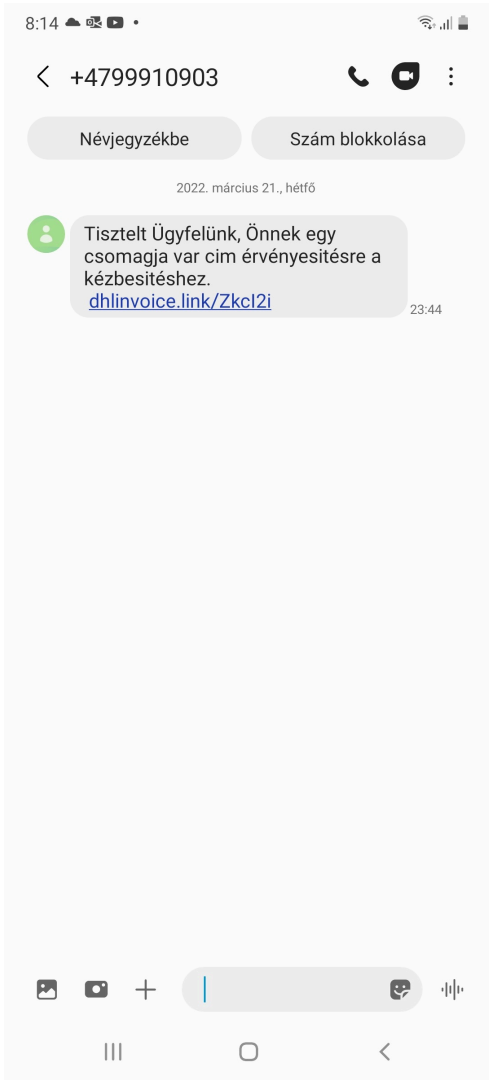
You have just two options. We should explore these types of options in details:

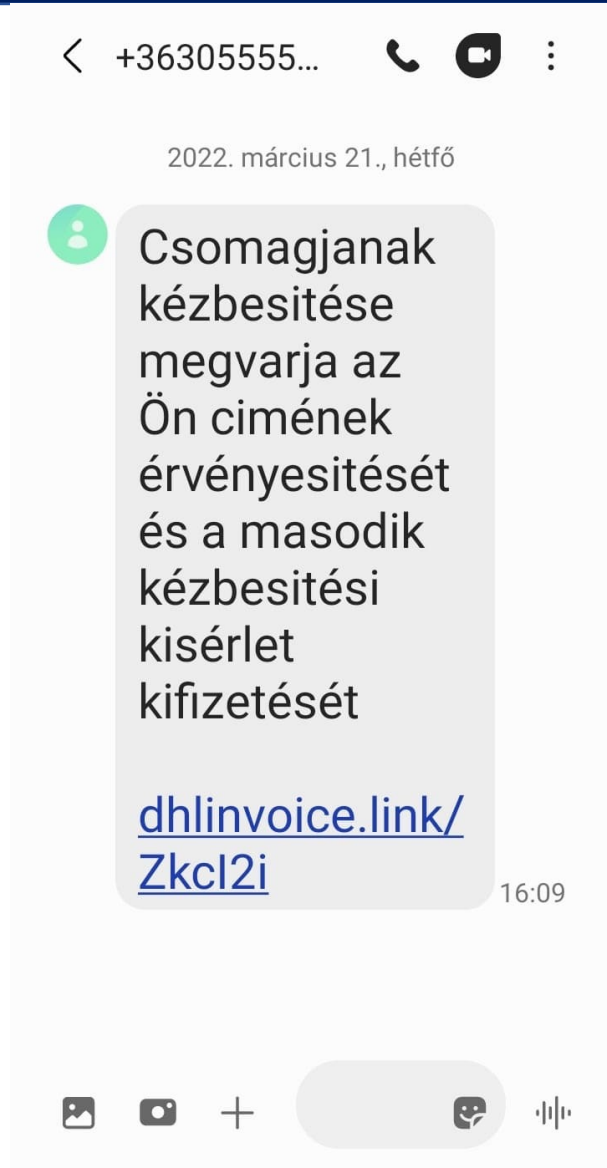
Very first choice is to just ignore this e-mail. As a consequence, I will send out your very own videotape to just about all of your contacts and also consider regarding the humiliation you will definitely get. Moreover in case you are in a committed relationship, just how it can affect?

Next choice should be to pay me $5000. Let us regard it as a donation. In this case, I most certainly will instantaneously eliminate your videotape. You will continue on with everyday life like this never occurred and you will not ever hear back again from me.

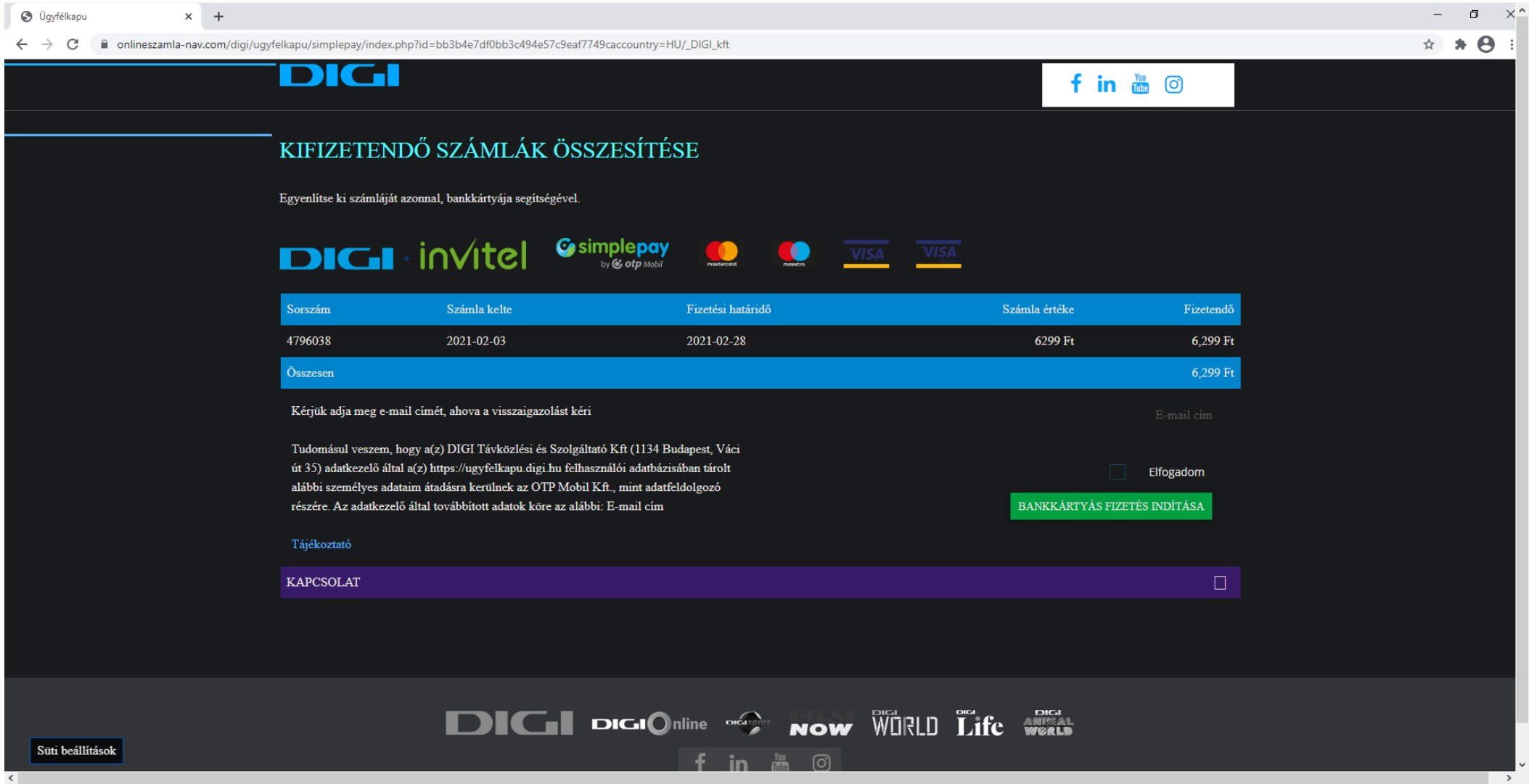
You will make the payment via Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google).

Phishing példák

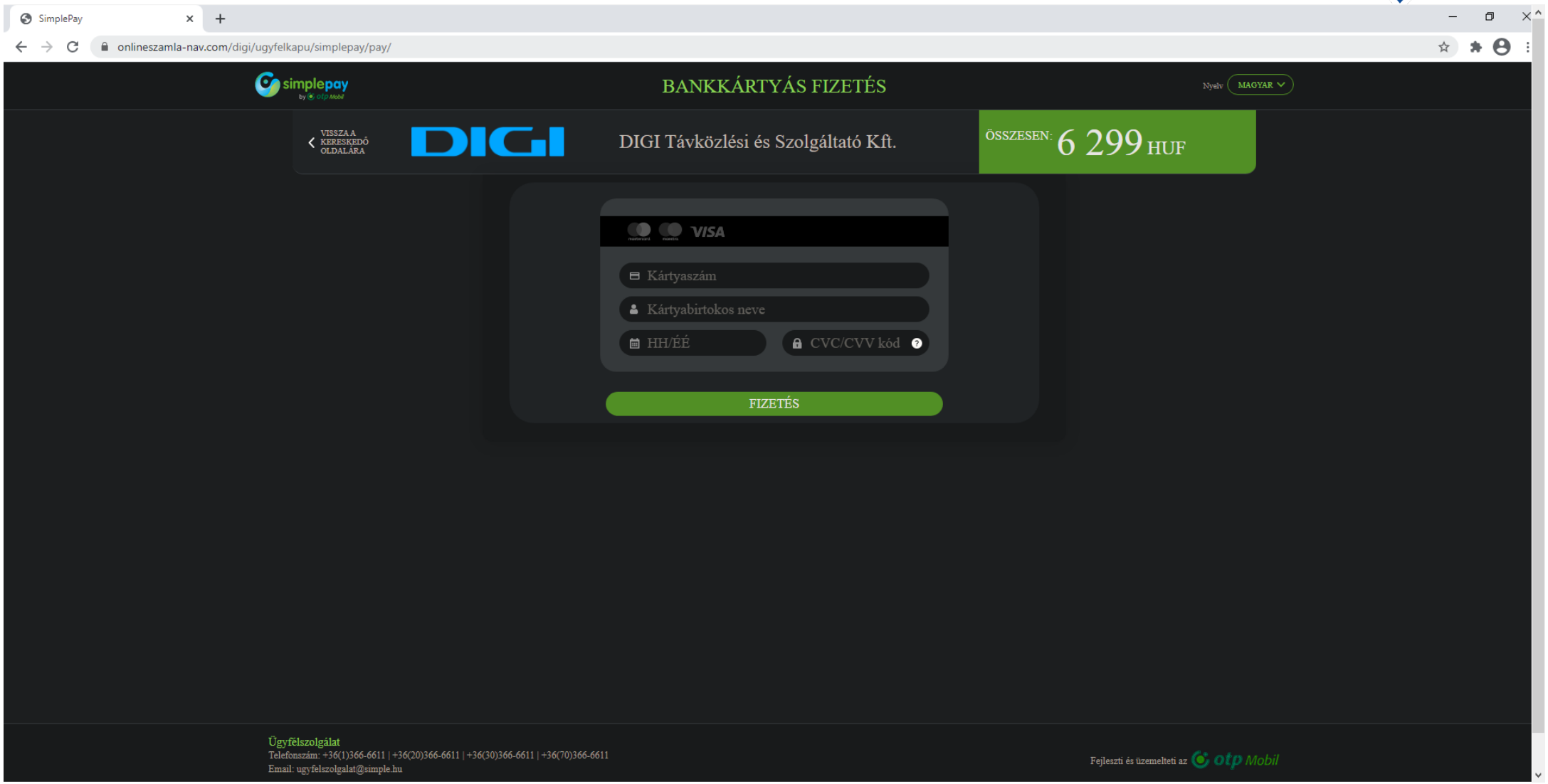




Phishing példák



Phishing példák



Phishing példák

From: DPD
Sent: Sunday, January 17, 2021 3:35 PM
To: budaventura@budaventura.hu lookup email lookup "budaventura.hu"
Subject: [ob6xp6dy1qvry98j]

Szia, budaventura@budaventura.hu lookup email lookup "budaventura.hu"

További részletekre van szükségünk a csomag újbóli kézbesítéséhez, mint a megadott cím hiányosnak tűnik.

Kérjük, adja meg a teljes információt ehhez a címhez, hogy megkísérelje az újratöltést.

Csomagját jelenleg a helyi raktárunkban tároljuk.

Ha azonban a művelet nem történik meg 48 órán belül, akkor azt visszaküldik az eredeti feladónak.

>>>>> Frissítse a visszaszállítási címet <<<<<

DPD @ 2021

Phishing példák

https://www.posta.hu.mitmom.com/flower774659/

Magánszemélyek | Üzleti partnerek | ÉnPostám | Belépés | Kosár (0) | HU

Magyar Posta

KÜLDEMÉNY FELADÁSA | KÜLDEMÉNY ÉRKEZÉSE | BE- ÉS KIFIZETÉS | PÉNZÜGYI SZOLGÁLTATÁSOK | KÖZMŰ ÜGYINTÉZÉS | BÉLYEG | ÚJSÁG | EGYÉB | WEBSHOP

Azonosító szám: 97357445

(Expressz csomag)

Fizetési részletek :

Címsor *

város *

postai

Teljes név *

telefonszám*

További szállítás

805,28 HUF

(Tartalmazza az ÁFÁt)

Teljes : **805,28 HUF**

(Tartalmazza az ÁFÁt.)

----------Eredeti üzenet----------

Dátum: 2022. február 23., szerda, 09:35:27

Feladó: "Magyar Posta."

Tárgy: A Magyar Posta tájékoztatta, hogy az Ön szállítása: 97357445HU

Címzett: undisclosed-recipients@ismeretlen

Tisztelt Ügyfelünk,

A Magyar Posta tájékoztatta, hogy az Ön szállítása: 97357445HU, és díjfizetésre vár

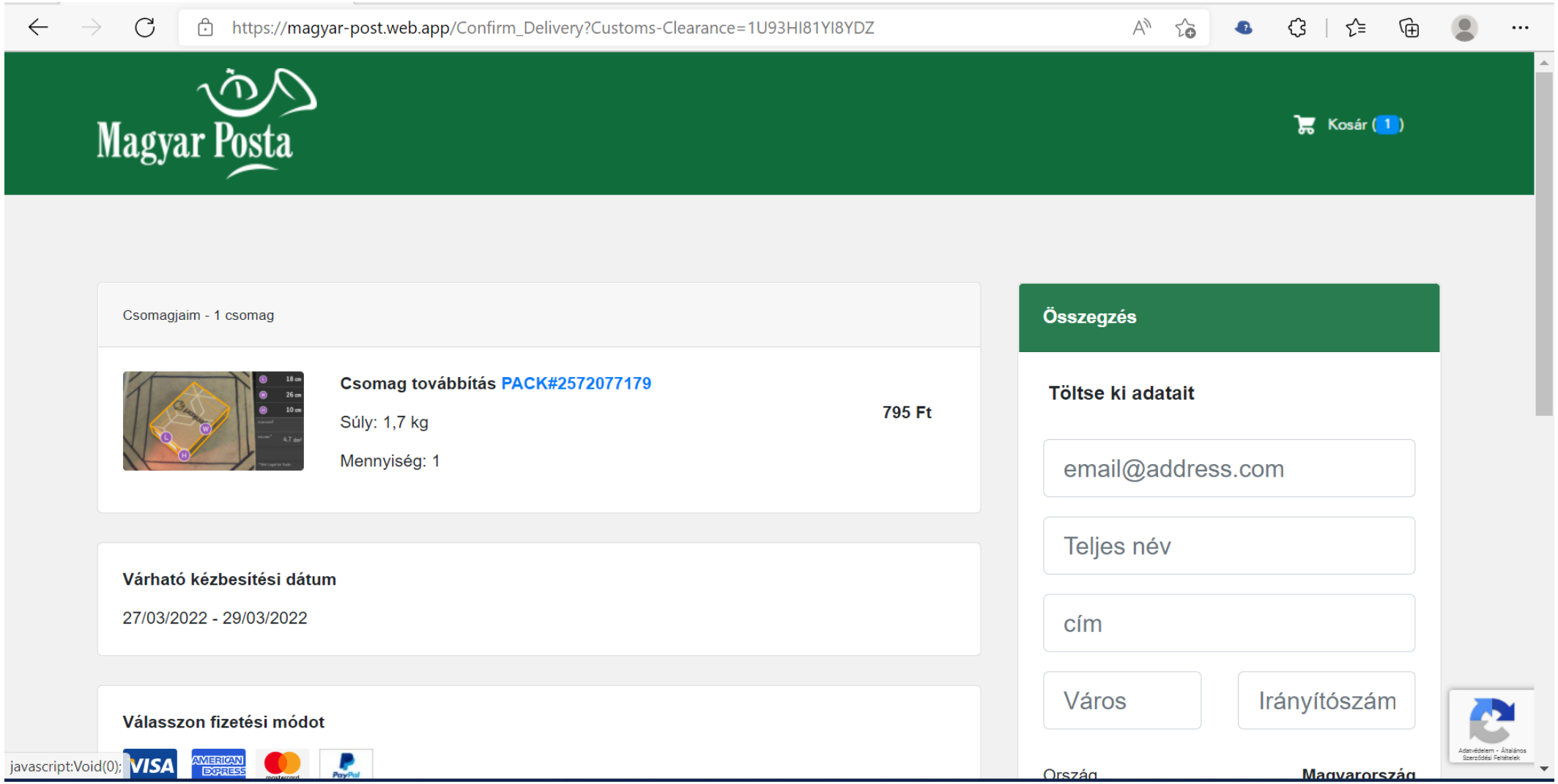
Díjak: 805,28 HUF

Dátum : 02/24/2022.

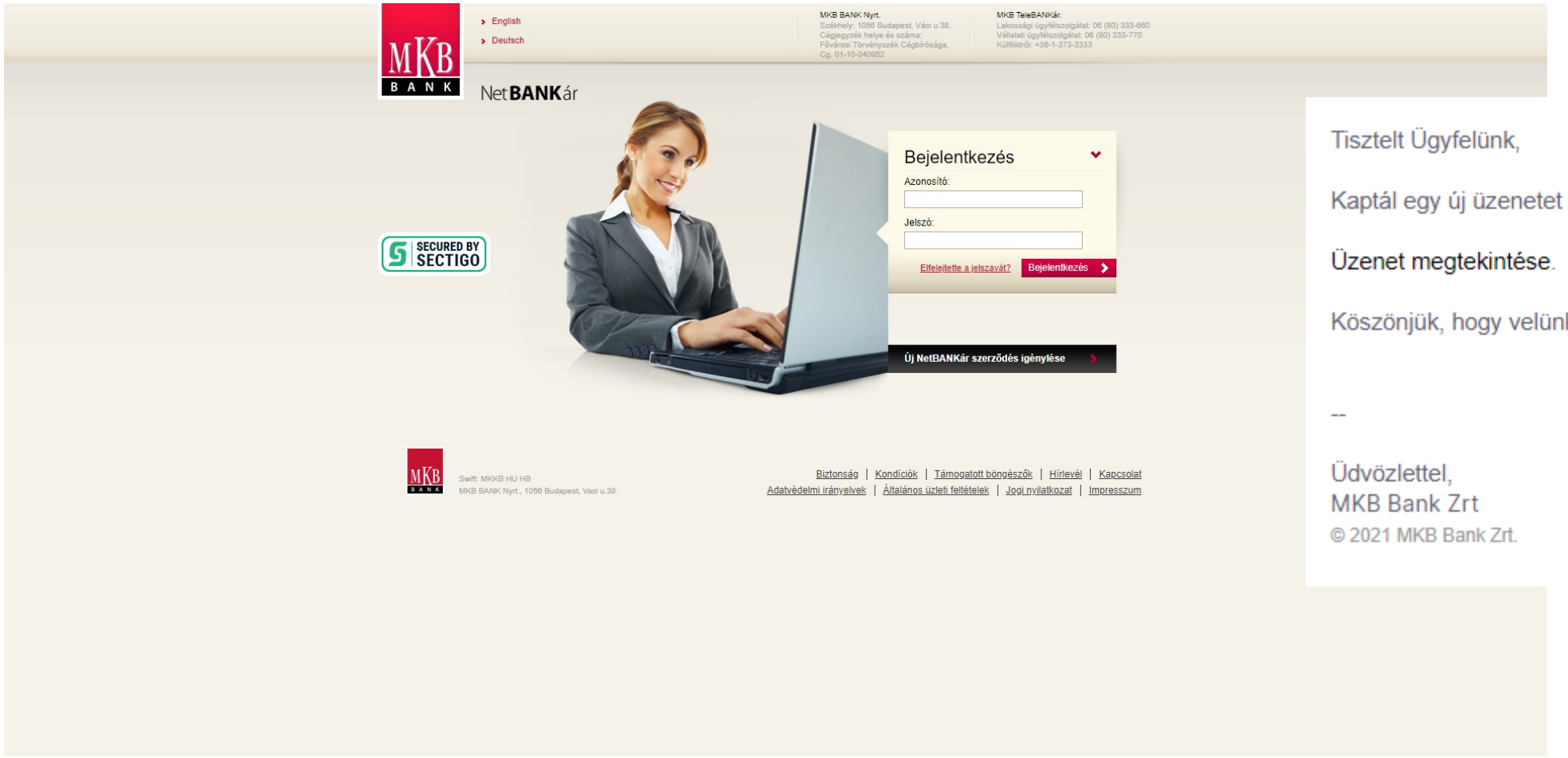
Küldd el a csomagomat

2022 © - Posta all rights reserved

Phishing példák



Phishing példák



Tisztelt Ügyfelünk,

Kaptál egy új üzenetet MKB Bank.

Üzenet megtekintése.

Köszönjük, hogy velünk Banking.

--

Üdvözlettel,
MKB Bank Zrt

Phishing példák

Tisztelt Ügyfelünk!

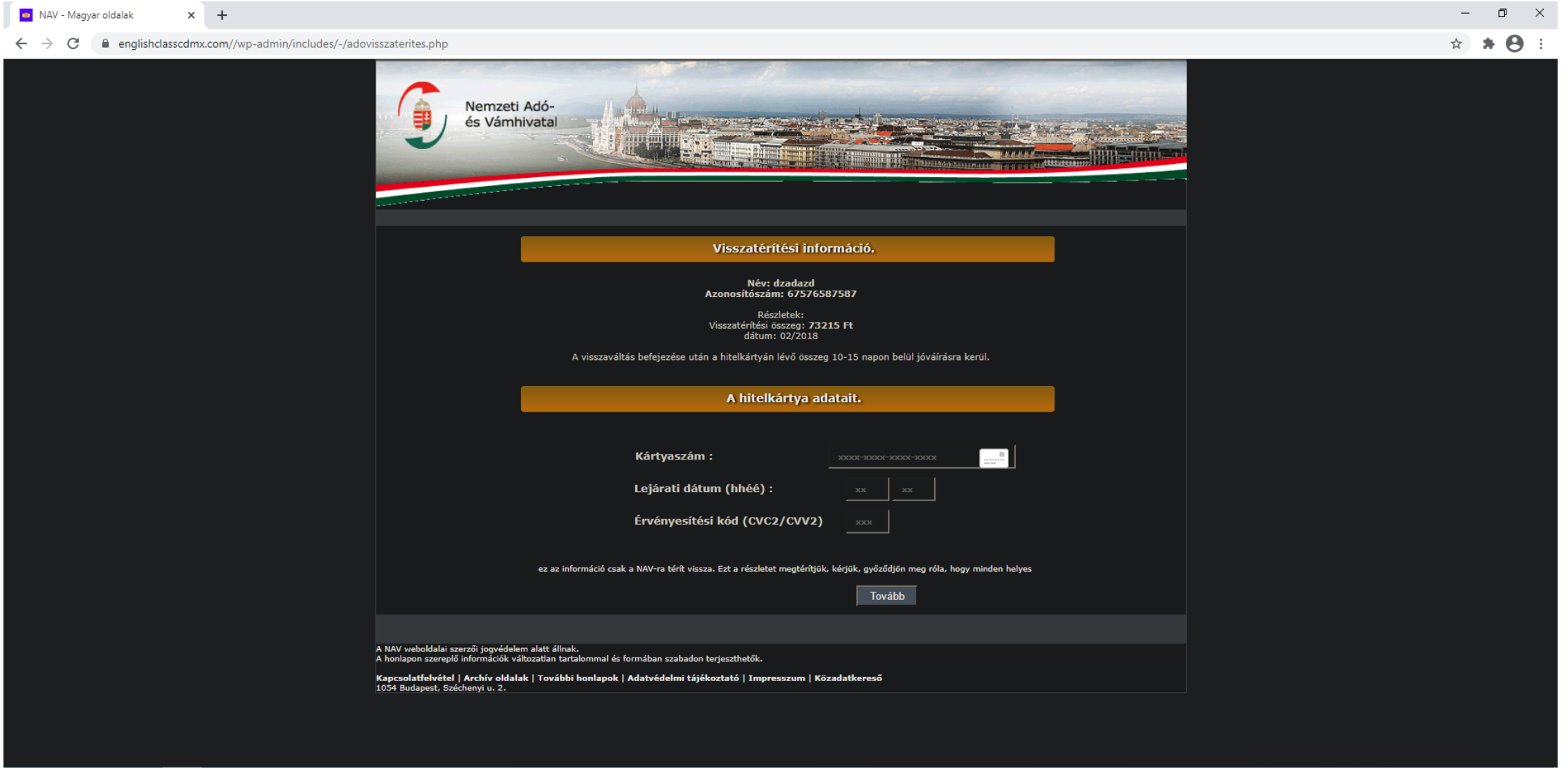
Az idén kifizetett összes adót az online ügyfelek számára ellenorizték. Az év végén jelentkezzen be az alábbi linkre, és hajtsa végre az alábbi lépéseket: Adja meg nevét, vezetéknevét és azonosítószámát, és erosítse meg e-mailjeit. Biztosítjuk, hogy jogod van az ebben az évben fizetett pénz visszaszerzésére

Ellenorizze most

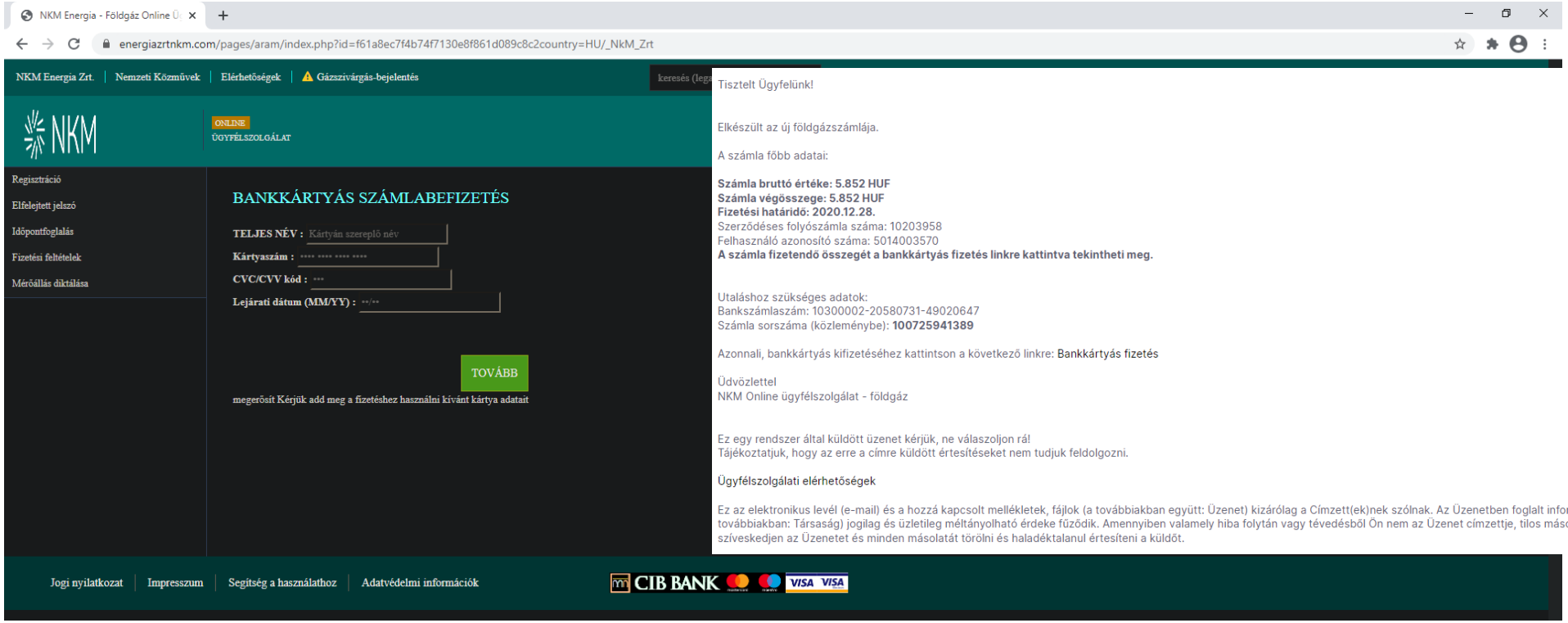
Kérem jelentkezzen be az adóvisszatéritési oldalra,hogy visszaigényelheti az alapokat.

Kiemelt figyelemre számíthatnak a virágot, koszorút és mécseseket árusítók. A NAV munkatársai a nyugta- és számlaadást, az online pénztárgép megfelelo üzemeltetését, valamint az alkalmazottak bejelentését vizsgálják.

Phishing példák



Phishing példák



Tisztelt Ügyfelünk!

Elkészült az új földgázszámlája.

A számla főbb adatai:

Számla bruttó értéke: 5.852 HUF
Számla végösszege: 5.852 HUF
Fizetési határidő: 2020.12.28.
Szerződéses folyószámla száma: 10203958
Felhasználó azonosító száma: 5014003570
A számla fizetendő összegét a bankkártyás fizetés linkre kattintva tekintheti meg.

Utaláshoz szükséges adatok:
Bankszámlaszám: 10300002-20580731-49020647
Számla sorszáma (közleménybe): **100725941389**

Azonnali, bankkártyás kifizetéséhez kattintson a következő linkre: Bankkártyás fizetés

Üdvözlettel
NKM Online ügyfélszolgálat - földgáz

Ez egy rendszer által küldött üzenet kérjük, ne válaszoljon rá!
Tájékoztatjuk, hogy az erre a címre küldött értesítéseket nem tudjuk feldolgozni.

Ügyfélszolgálati elérhetőségek

Ez az elektronikus levél (e-mail) és a hozzá kapcsolt mellékletek, fájlok (a továbbiakban együtt: Üzenet) kizárólag a Címzett(ek)nek szólnak. Az Üzenetben foglalt információk bizalmasak lehetnek, melyeknek titokban maradásához az NKM Energia Zrt.-nek (a továbbiakban: Társaság) jogilag és üzletileg méltányolható érdeke fűződik. Amennyiben valamely hiba folytán vagy tévedésből Ön nem az Üzenet címzettje, tilos másolnia, továbbítania, közölnie vagy bármely részét felhasználnia. Ebben az esetben szíveskedjen az Üzenetet és minden másolatát törölni és haladéktalanul értesíteni a küldőt.

Phishing példák

Tisztelt Ügyfelünk!

Elkészült az új földgázszámlája.

A számla főbb adatai:

Számla bruttó értéke: 1.340 HUF
Számla végösszege: 1.340 HUF
Fizetési határidő: 2021.01.15
A számla fizetendő összegét a bankkártyás fizetés linkre kattintva tekintheti meg.
A számla részletes adatait a NKM Online Ügyfélszolgálat Számlázás - Számlák lekérdezése menüpontban tekintheti meg.

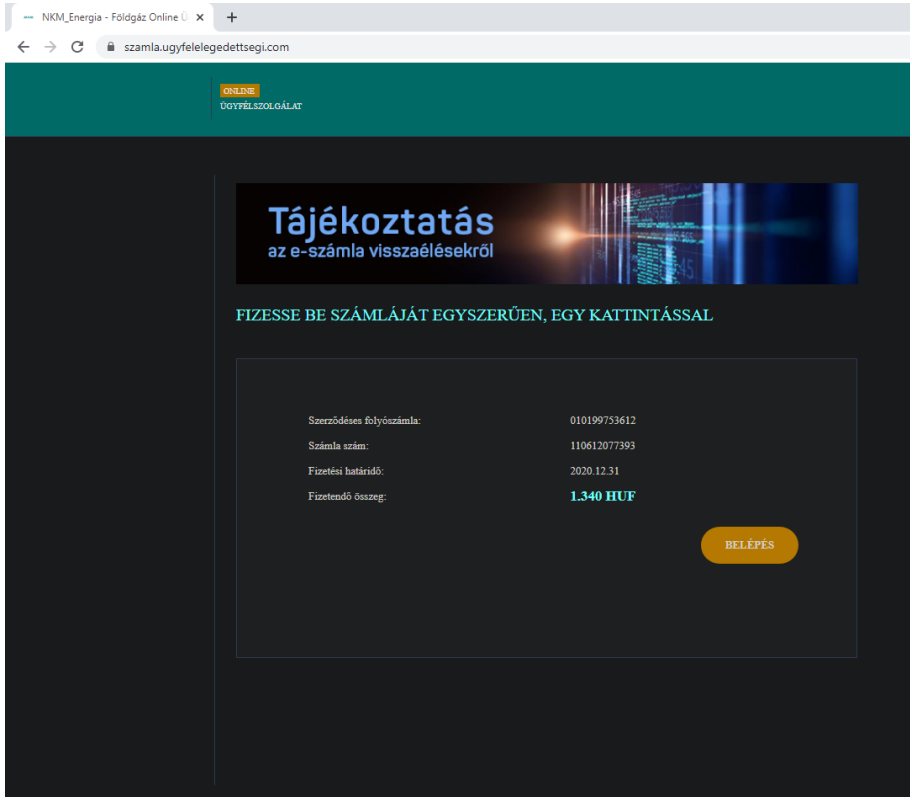
Azonnali, bankkártyás kifizetéséhez kattintson a következő linkre:
Bankkártyás fizetés

Esetleges kérdésével forduljon bizalommal ügyfélszolgálatunkhoz!

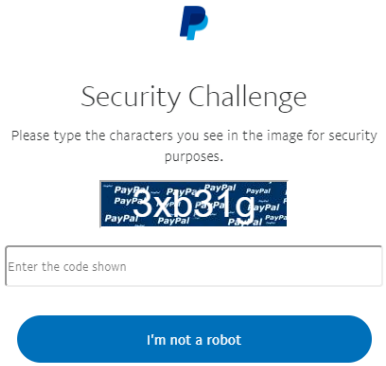
Üdvözlettel
NKM Online ügyfélszolgálat - földgáz

Ez egy rendszer által küldött üzenet kérjük, ne válaszoljon rá!
Tájékoztatjuk, hogy az erre a címre küldött értesítéseket nem tudjuk feldolgozni.

Ügyfélszolgálati elérhetőségek



Phishing példák



HU

PayPal

Jó nap,

Tranzakciós kérelmet kaptunk pénz befizetésére az alább felsorolt online pénztárcákban

Skrill és Neteller a kártyád használatával, amely összekapcsolódott a PayPal-számláddal. Ezért volt

tegye vissza a tranzakciós kérelmet, és 48 órán keresztül adjon hozzá korlátozást PayPal-számlájához.
Ha Ön volt a tranzakció tulajdonosa, kérjük, ne csináljon semmit, és hagyja figyelmen kívül ezt az üzenetet.

A PayPal mindkét pénztárca visszaigazolja a tranzakciós utalást (Skrill és Neteller)

ha nem, kérjük, kövesse ezeket a következő lépéseket az ügylet visszavonásához és az azonnali visszatérítés kéréséhez

Fontos figyelmeztetés: automatikus rövid üzenetet küld a telefonszámra, amely tartalmazza egy kód a jogosulatlan tranzakció törlési folyamatának befejezéséhez.

A visszatérítés iránti kérelem teljesítéséhez be kell írnia az SMS-kódot, a kódot

tartalmazza a felhasznált összeget.

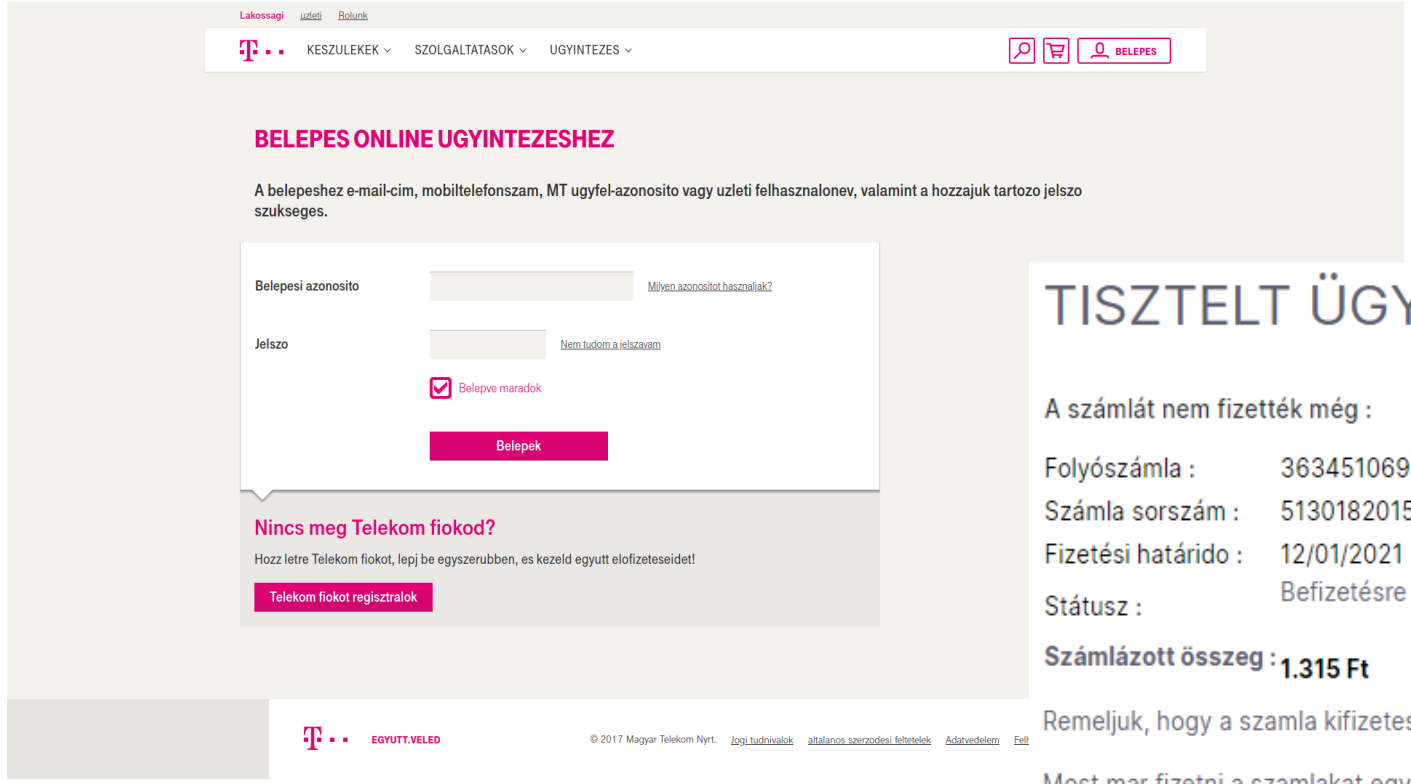
Az alábbi linkre kattintva törölnie kell a tranzakciót és kérnie kell a visszatérítést.

Vissza a pénzemet

Figyelem: Ez az e-mail automatikusan jön létre, és nem az ügyfél és a PayPal közötti kommunikációra szolgál.

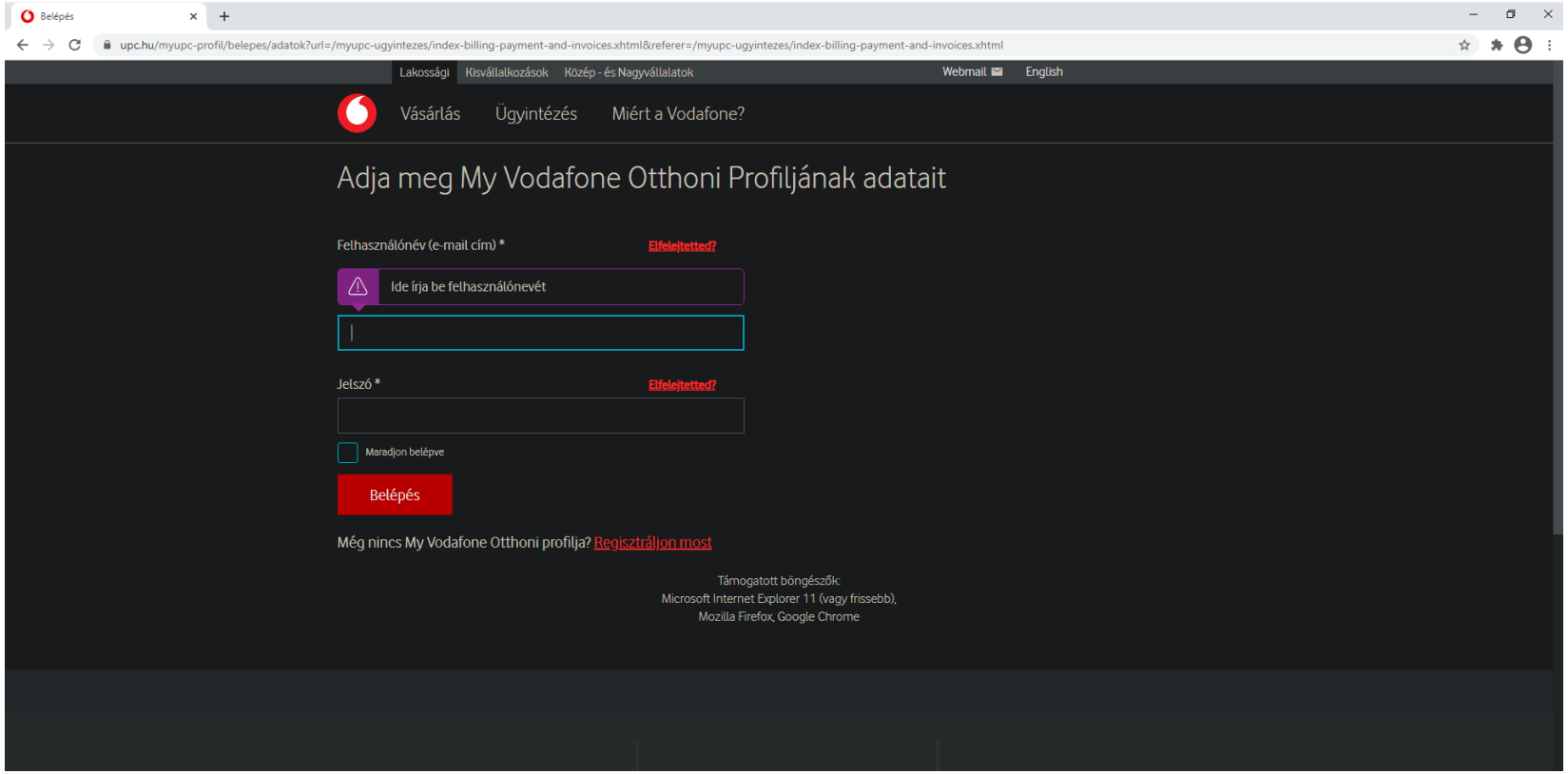
Köszönöm a megértést

Phishing példák



Phishing példák

Phishing példák



Kedves Ügyfelünk!

Aktuális havi (korábbi UPC vezetékes vagy mobilszolgáltatás) elektronikus számlád elkészült, melynek részleteit az alábbiakban küldjük számodra.

Amennyiben számládat már rendezted, kérjük, üzenetünket tekintsd tárgytalannak.A csekkes befizetés 3-4 munkanap, az utalás 1-2 munkanap amíg könyvelődik.

Számla alapján fizetendő: 14889Ft

Fizetési határidő: 2020-12-29

Számla kelte: 2020-12-11
Számla sorszáma: 834813026
Ügyfélszám: 0029126380
Iktatószám: CC-5865118/2-2020

A számla összege az aktuális havi tételek összegét tartalmazza, az esetleges korábbi túlfizetéseidet vagy számlaelmaradásaidat nem.

Kérjük, ne feledd, hogy amennyiben e-Pack tarifával rendelkezel, a kedvezmény igénybevételének feltétele, hogy a fizetendő összeget internetes bankkártyás fizetéssel, átutalással, OTP bankautomatán keresztül vagy csoportos beszedési megbízással egyenlítsd ki Banki átutalás esetén a(z) 10410022002912638000010 2 számlaszámot használd, a közlemény mezőben tüntesd fel az ügyfélszámodat: 0029126380.

Elérhetőségeink

E-mail: www.vodafone.hu lookup host /kapcsolat
Telefonszám: 1270
Külföldről hívható telefonszám: +36 1 288 1270
Levelezési cím: 1476 Budapest Pf.303

Üdvözlettel:
Vodafone

Ezt a levelet a Vodafone Magyarország Zrt. küldte tájékoztató jelleggel. A Szolgáltató az adataidat bizalmasan kezeli. A levél tartalmáért a Szolgáltató felelős.

Személyes adataid kezeléséről további információért keresd fel a Vodafone Adatvédelmi

Zsarlóvírusok

- Zsarlóvírus: A zsarolóvírus egy olyan típusú **támadás**, amelyben a támadók átveszik az **irányítást** a célpont eszközei felett, és **váltságdíjat** követelnek cserébe az **eszköz elérhetőségének visszaállításáért** és titkosságáért.

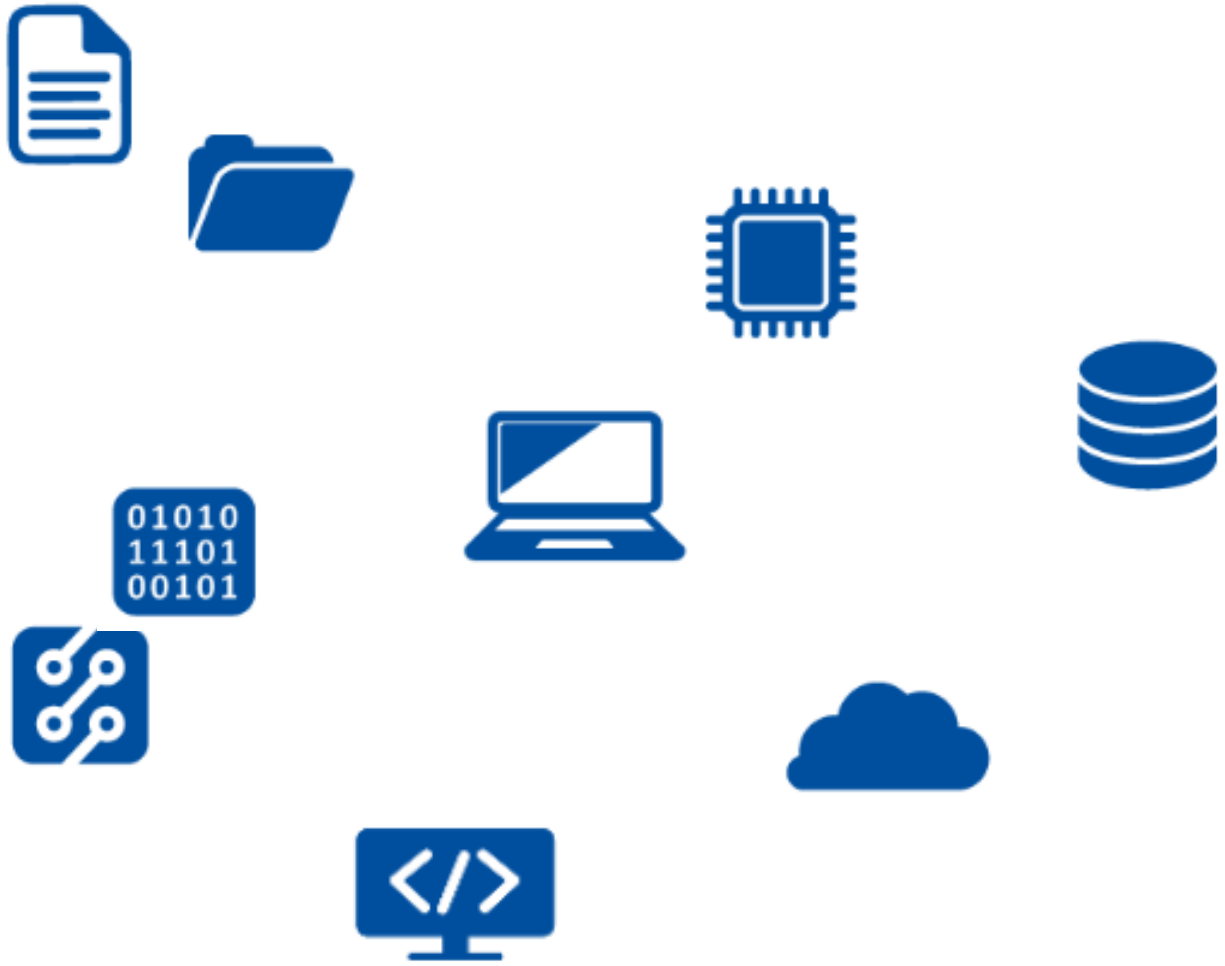
Zsarlóvírusok típusai

A zsarolóprogramok négy alapvető műveletet hajthatnak végre:

- zárolás
- titkosítás
- törlés
- lopás

Zsarolóprogram által megcélzott előforrások

- Fájlok
- Mappák
- Memória
- Adatbázis
- Kijelző
- MFT
- MBR
- Felhő
- CMS



Zsarolóvírus életciklusai

- Kezdeti hozzáférés
  - hozzáférés megszerzése
  - biztonsági szoftver letiltása
  - helyreállítási funkciók leállítása
  - zsaroló program telepítése

Zsarolóvírus életciklusai

- **Végrehajtás**
  - célpont tanulmányozása
  - további gépekre terjedés

Zsarolóvírus életciklusai

- **Cél** megvalósítása
  - Eszköz elérhetőségének vagy titkosságának megtámadása

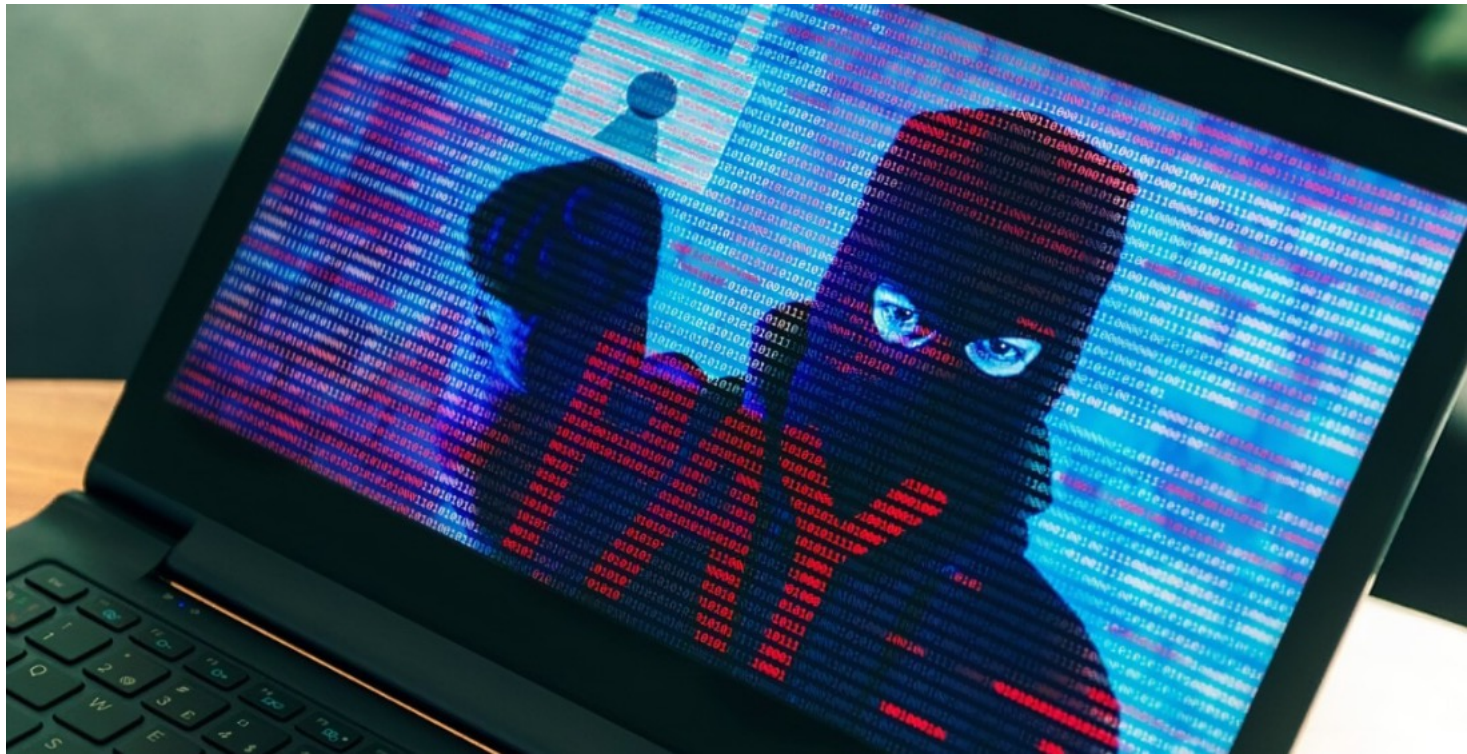
Zsarolóvírus életciklusai

- **Zsarolás (ransom)**
  - Kommunikáció
  - Fenyegetés
  - Követelés

Váltságdíj tárgyalások

- Privát kommunikáció a célpont és a támadó között (nem ajánlott lépés)

- Két kimenetel:
  - Célpont kifizeti a váltságdíjat
  - Nem fizeti ki a célpont a váltságdíjat



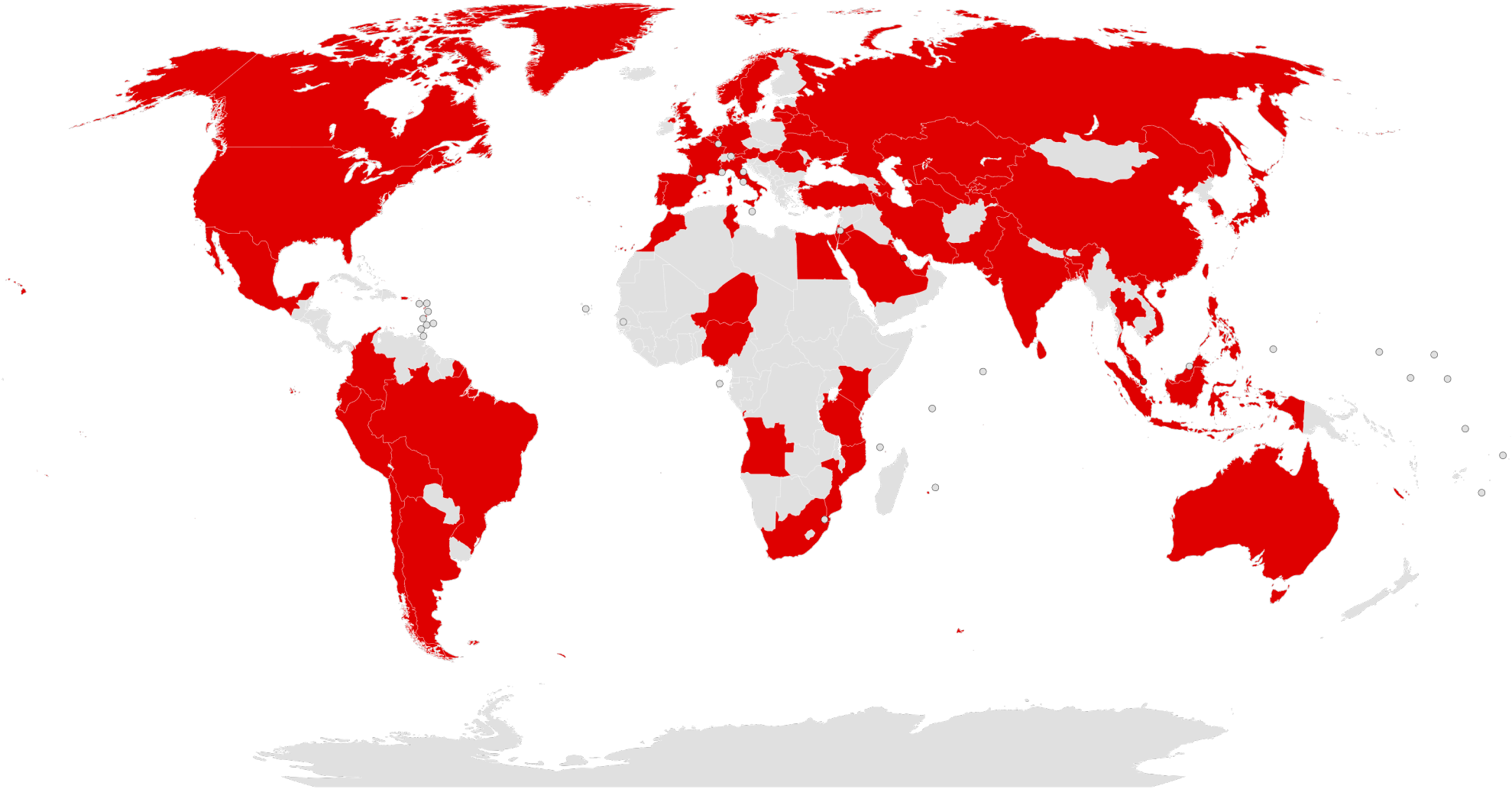
Zsarolóvírus terjedése

- „Szokásos módon”
  - E-mailben
  - Csatolmány vagy URL segítségével
  - Sérülékenység kihasználásával
- Új támadási formák
  - RDP-n keresztül
  - TeamViewer segítségével
  - Nem titkosítanak – jelszavas archívek használata
    - Az alkalmazás rendelkezésre áll a szerveren
    - A károkozás így is megtörténik

A leghíresebb

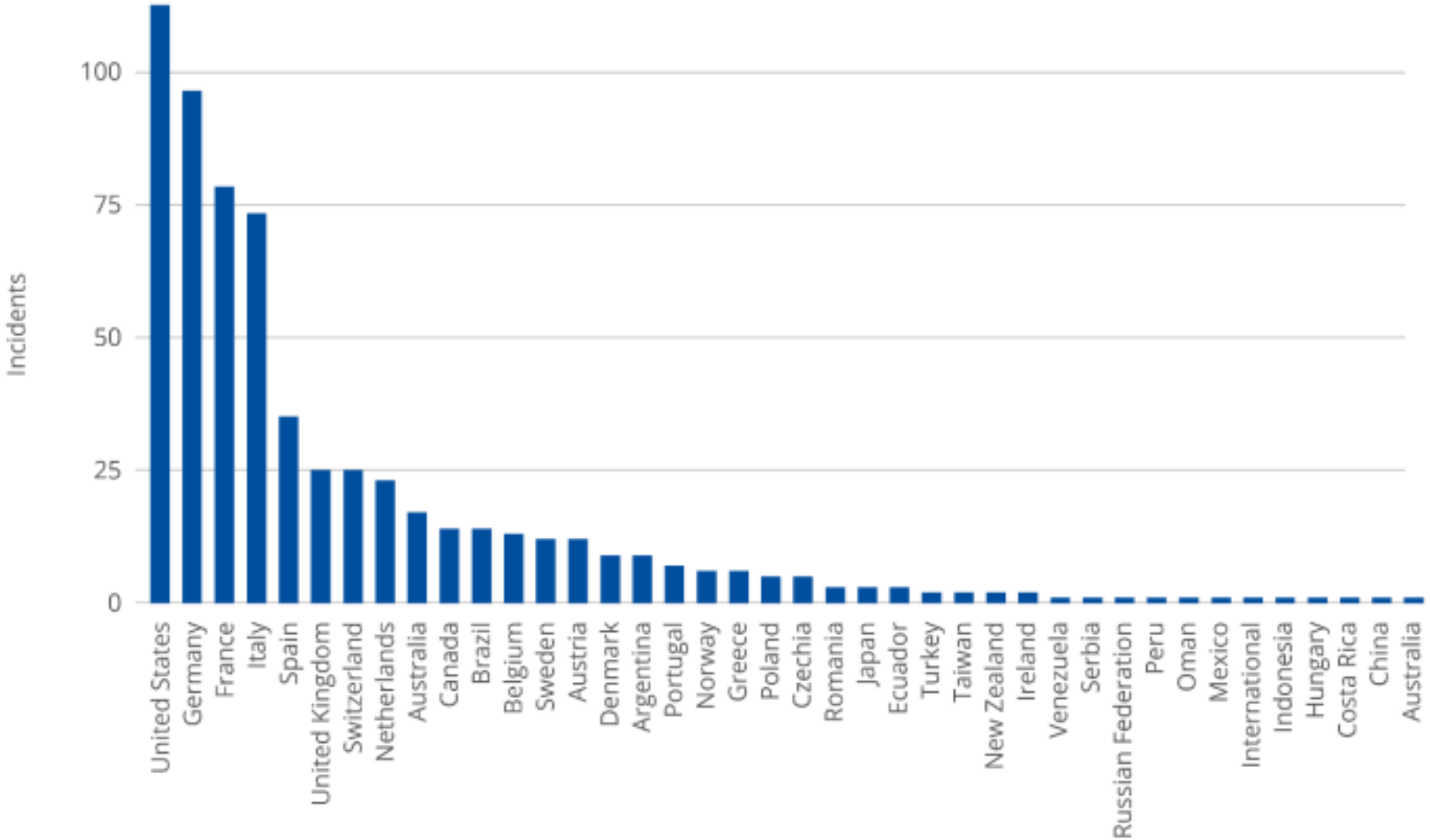
- Wanacry 2017
- Kb 230 000 áldozat 4 nap alatt
- Lazarus csoport - KNDK
- Windows SMB sérülékenység
- Ethernal blue – NSA
- Áldozatok (milliárd dollár)
  - Nissan
  - Renault
  - Tekefónica
  - FedEx
  - Deutche Bahn
- Kill switch (titkosítás és terjedés)

A leghíresebb



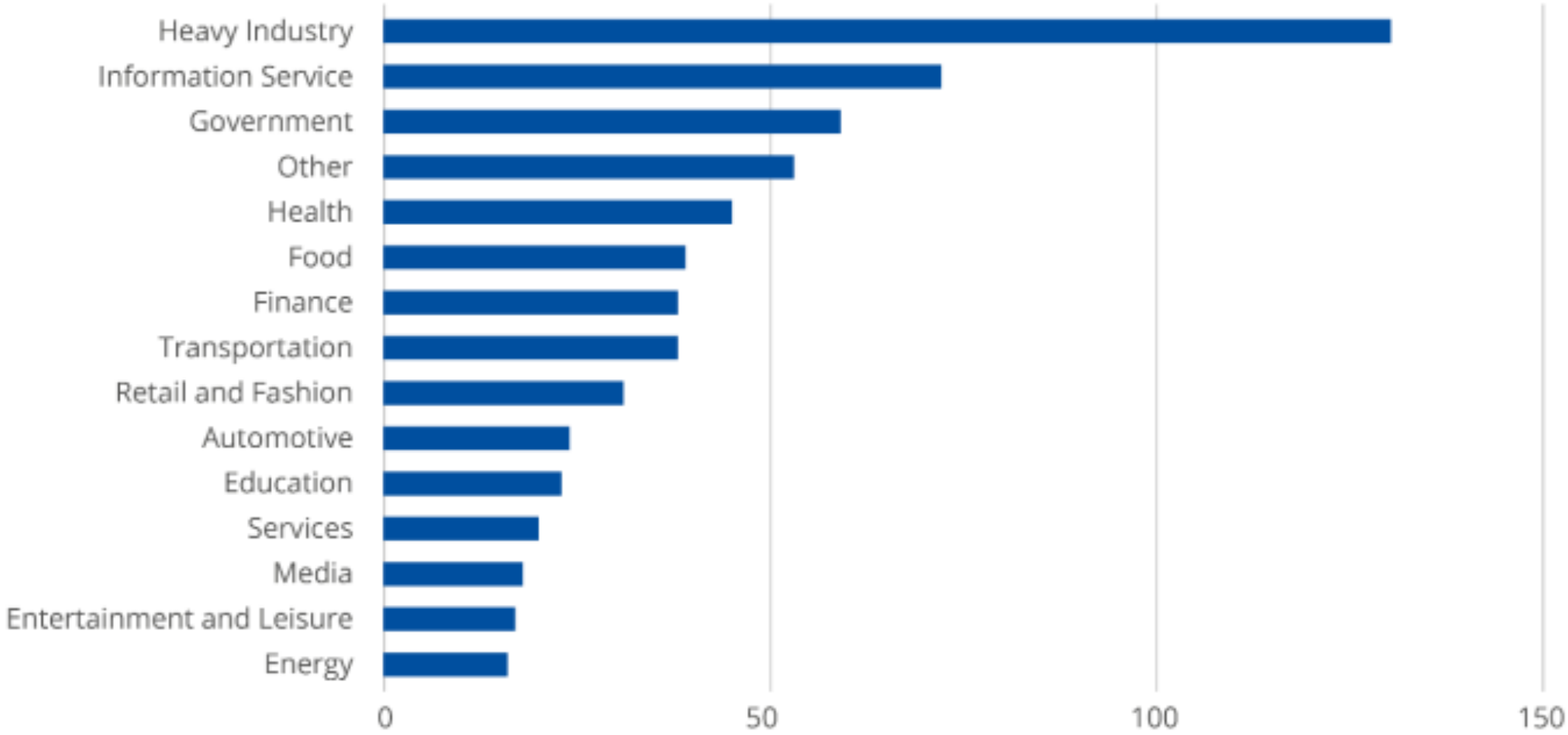
Zsarolóvírus incidensek analízise

- A zsarolóvírus incidensek száma országonként 623 elemzett incidens alapján

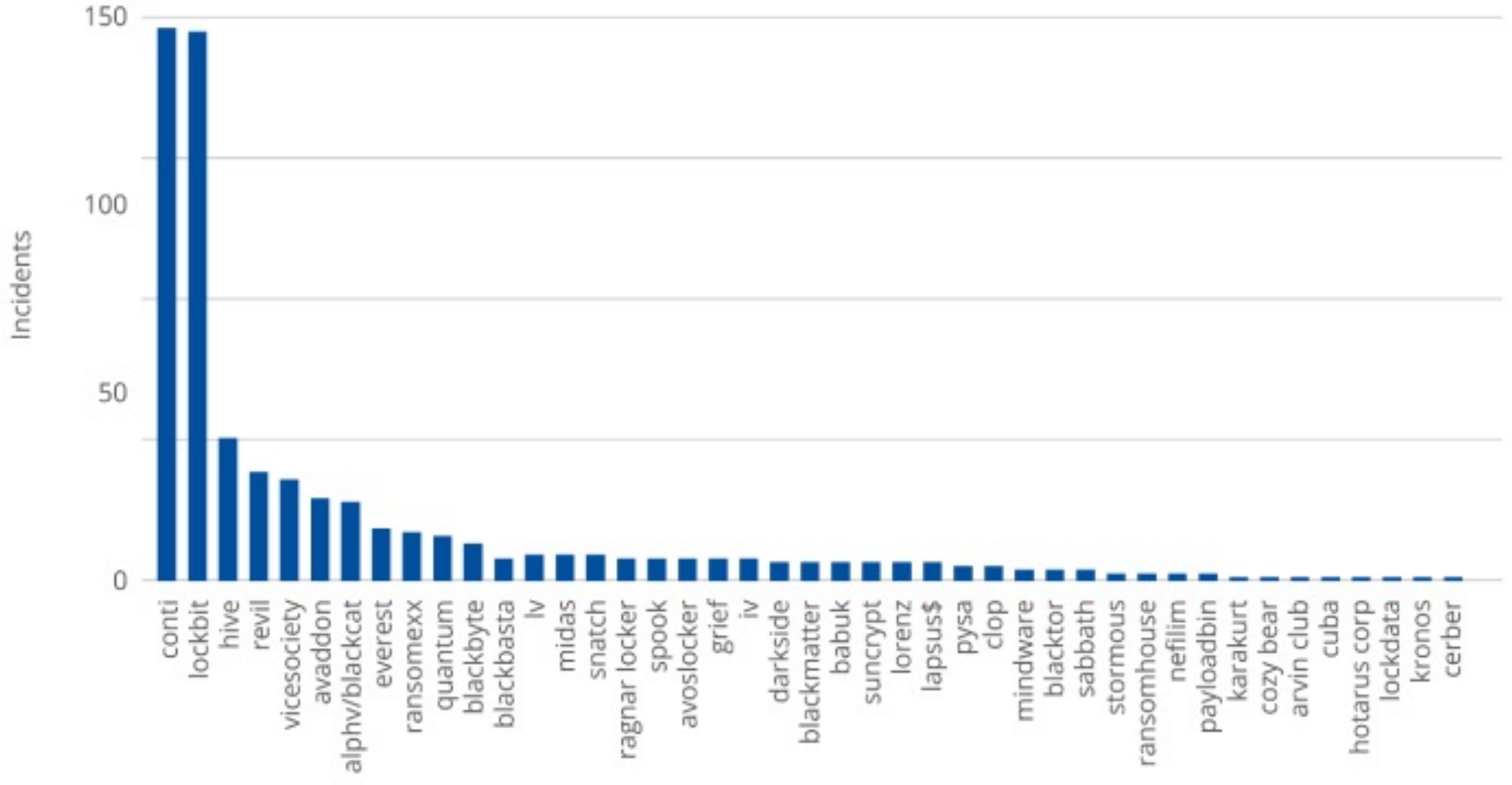


Zsarolóvírus incidensek analízise

- A zsarolóvírus incidensek számának összehasonlítása az egyes ágazatokban



Zsarolóvírus incidensek analízise



Ajánlások

- Ellenőrzött, naprakész **biztonsági mentés** ami a hálózattól el van szigetelve
- Alkalmazza a **biztonsági mentés 3-2-1** szabályát.
- A **személyes adatokat** a GDPR rendelkezéseinek megfelelően **titkosítva tárolja**, és használja a megfelelő kockázatalapú ellenőrzéseket
- **Biztonsági szoftver** futtatás
- **Biztonságtudatosság** naprakészen tartása
- Kockázatértékelések
- Rendszergazdai jogok korlátozása

Megelőzés

- Csak ellenőrzött forrásból telepítsünk
- Ismeretlen feladótól származó e-maileket ne nyissunk meg
- Biztonsági mentés készítés hetente, naponta

Reagálás zsarolóvírusokra

- Forduljon a Nemzeti Kibervédelmi Intézethez
- Ne fizessen váltságdíjat
- Az érintett rendszereket helyezze karanténba
- Később még lehet feloldása a zsarolásnak

Köszönöm a figyelmet!

csirt@nki.gov.hu

Kibertámadás! Podcast

nki.gov.hu